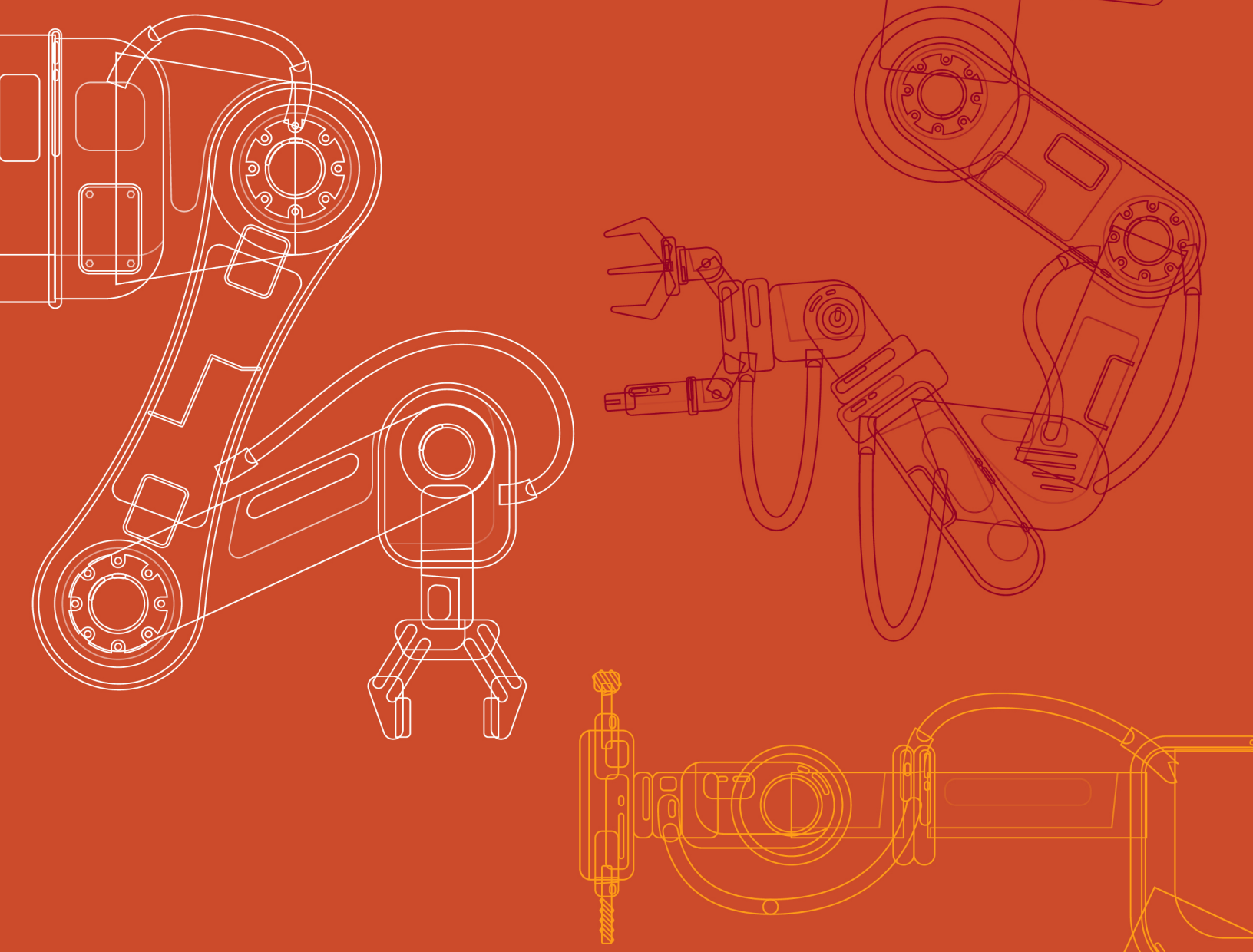


HUSCH BLACKWELL

Legal Insights for Manufacturing

A look ahead at the issues that will shape 2025 for the manufacturing industry

OCTOBER 2024

Introduction

Intensifying international crises, increasing regulatory burdens, and uncertain macroeconomic conditions have led to an era of caution for manufacturers, but hidden among those challenges are exciting opportunities for growth.

Nothing makes business leaders more uneasy than uncertainty. Change is okay—indeed, it is axiomatic—but not being able to get in front of change and manage it can be a frustrating prospect. Many manufacturing companies are encountering disruption on a scale that was unfathomable a generation ago and that affects nearly every area of operations, from trade, transportation and logistics to workforce structure and corporate finance.

Taken singly, the developments and trends we're watching—including supply-chain reconfiguration, the energy transition, major administrative and regulatory law changes, shifts in the credit cycle, and fluctuating consumer demand, among others—would be big news items. But these developments are occurring together and are often impacting one another. Pundits call it *polycrisis* when concurrent crises overlap and reinforce each other, and although the term has existed since the 1980s, recent events have elevated it to something of a buzzword over the past few years—for good reason. However, we also believe that the uncertainty provides nimble businesses with incredible opportunities for growth if the uncertainty is met head on.

Aside from the challenges noted above, we are also contending with wildcard events that no one can predict. For instance, when 2024 draws to a close, a record-number of people worldwide—some two billion—will have headed to the polls to cast ballots in national elections, including here in the United States. The results of these political contests around the globe will surely influence the established trend lines, but it is difficult to know with any degree of certainty how election outcomes might impact the cluster of disparate crises that are already in play, or how they might lead to new crises that have yet to emerge.

With our third-annual *Legal Insights for Manufacturing* report, we have chosen to highlight areas of concern that we believe transcend day-to-day electoral politics and that are poised to exert influence on the way manufacturers develop their strategies to compete well into the future. We hope the perspectives captured here can help clear away some of the fog associated with polycrisis and provide industry leaders with creative, practical insights that lead to success.

Jeffrey Sigmund

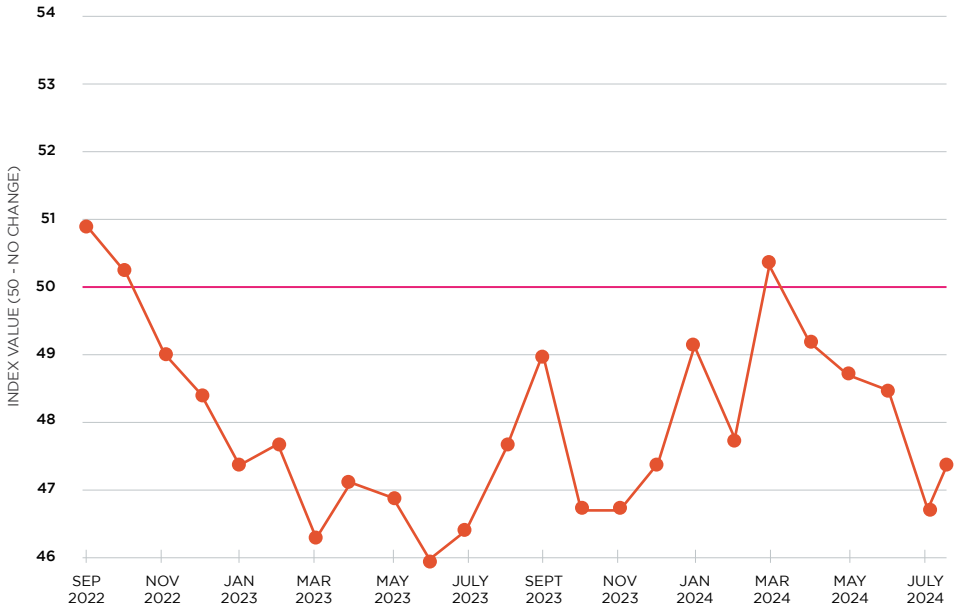
Head of Husch Blackwell's Technology, Manufacturing & Transportation Group

Setting the Agenda

Manufacturing industry sentiment continues to trend below its historical average. Traditional sources of worry—the scarcity of labor and the increasing cost of regulatory compliance—remain at the top of the list; however, economic and demand-related concerns are mounting as 2024 comes to a close.

According to the **Institute for Supply Management**, the manufacturing industry finally registered a month of economic expansion in March 2024, but as of midyear, it has reverted to prior performance and has now contracted in 20 of the preceding 21 months. This is the longest sustained period of industry contraction since the Global Financial Crisis of 2008-09 and one of the longest stretches of industry contraction on record. Such data are typically seen within the context of a wider economic recession, but the U.S. economy has posted a positive GDP every quarter since early 2022. This broken correlation likely explains industry sentiment, which is generally positive (but less so than the historical average). Nearly 72 percent of respondents to the National Association of Manufacturers' (NAM) latest **business outlook survey** were positive about their companies' outlook.

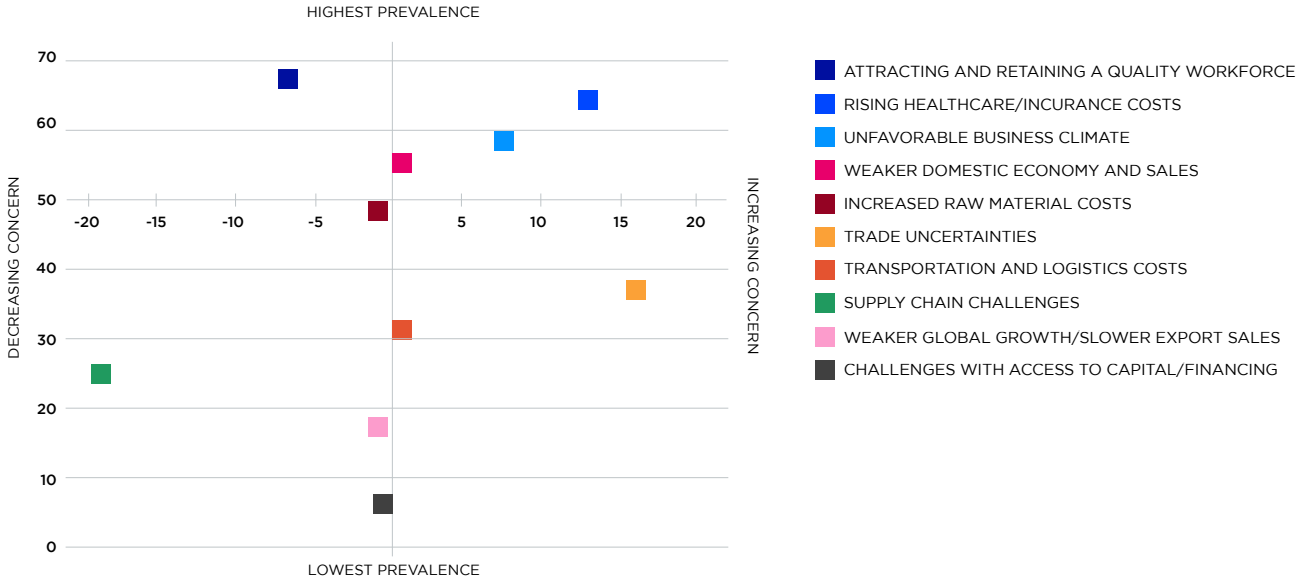
U.S. MANUFACTURING PURCHASING MANAGERS' INDEX
SEPTEMBER 2022 TO AUGUST 2024



Source: Institute for Supply Management.

Nevertheless, the survey identified a handful of areas where concerns are growing, including international trade, the cost of healthcare insurance, macroeconomic conditions, government regulation, and tax. That is in addition to the lingering impact of inflation, which is moderating but still running hotter than the Federal Reserve's two-percent target. For many manufacturers, interest-rate policy is a second-order concern, but its indirect effects can have a powerful influence on demand, which will be closely watched as we head into 2025.

PRIMARY CURRENT BUSINESS CHALLENGES



Source: *National Association of Manufacturers, NAM Manufacturers' Outlook Survey (June 26, 2024).*

Towering above all of these factors—especially in the popular imagination—is November's election season. No doubt the results of the election, both at the top and down-ticket, will have significant consequences for public policy, most notably in the areas of energy, taxes, and foreign policy; however, a glance at recent history suggests that the vagaries of electoral politics have had little impact on the growth of federal regulation, which continues unabated from administration to administration. We do not foresee this long-term trend reversing itself in 2025, no matter who prevails in November and despite recent Supreme Court decisions—like *Loper Bright, Corner Post*, and *Jarkesy*—that some believe will rein in the authority of administrative agencies.

Table of Contents

Regulatory & Compliance

GREGG N. SOFER AND REBECCA FURDEK

Federal and state administrative agencies continue to push out burdensome regulations and rulemakings, even as the U.S. Supreme Court wrapped up an historic term filled with decisions that some believe could limit administrative power in the future.

In prior reports we have noted how federal and state regulation falls most heavily on manufacturers, particularly those in the middle market. According to an **October 2023 study from the National Association for Manufacturers**, the per-employee cost of compliance with federal regulation exceeds $50,000 for manufacturing firms with less than fifty employees, more than double the cost for large firms.

Additionally, the intensity of regulatory oversight is growing. Over 90,000 pages—filled with new rules, regs, and guidance—were added to the Federal Register in 2023, the second-highest figure in history. As one might imagine with such a large—and largely uncoordinated—expansion of oversight, agencies frequently issue rules that are ambiguous, duplicative, or contradictory, adding significant complexity to the compliance function.

DOJ's New Whistleblower Program

Speaking of duplication and contradiction, the U.S. Department of Justice (DOJ) announced a **new whistleblower pilot program** in August 2024 after a soft launch in a **March speech** by Deputy Attorney General Lisa Monaco. The program purports to fill "gaps" between existing government whistleblower programs, but even before the program was finalized over the summer, private businesses voiced concerns about how it could undermine previous efforts by DOJ to encourage voluntary self-disclosure.

In 2023 DOJ's Criminal Division revised its Corporate Enforcement Policy (CEP) to incentivize companies to self-disclose illegal conduct. At its core, the update used the Department's prosecutorial discretion as a bargaining chip with private businesses. Declinations would depend on three factors: voluntary self-disclosures of misconduct, full cooperation, and timely remediation of the misconduct. This framework energized corporate compliance teams to establish processes and procedures to ensure timely self-reporting inside organizations, and it largely cohered both with DOJ's recent focus on individual responsibility and building properly resourced and fully functioning compliance programs.

The whistleblower pilot program cuts in the opposite direction, providing employees with incentives to bypass internal compliance programs altogether and take information to the government in the first instance, but there are notable limitations. Whistleblowers must be individuals; no companies or other entities are eligible. The individual must voluntarily offer "original information," which is defined as "derived from the individual's independent knowledge or independent analysis." The disclosure cannot be founded in publicly available information and cannot be already known by DOJ, and whistleblowers must fully cooperate with DOJ after divulging information.

DOJ CORPORATE WHISTLEBLOWER AWARD PROGRAM ELIGIBLE SUBJECT MATTER AREAS

FINANCIAL INSTITUTIONS

"Violations by financial institutions, their insiders, or agents, including schemes involving money laundering compliance violations, registration of money transmitting businesses, and fraud statutes, and fraud against or non-compliance with financial institution regulators."

FOREIGN CORRUPTION & BRIBERY

"Violations related to foreign corruption and bribery by, through, or related to companies, including violations of the Foreign Corrupt Practices Act, violations of the Foreign Extortion Prevention Act, and violations of the money laundering statues."

DOMESTIC BRIBERY & KICKBACKS

"Violations committed by or through companies related to the payment of the bribes or kickbacks to domestic public officials, including but not limited to federal, state, territorial, or local elected or appointed officials and officers or employees of any government department or agency."

HEALTHCARE

"Violations related to (a) federal health care offenses and related crimes involving private or other non-public health care benefit programs, where the overwhelming majority of claims are submitted to private or other non-public health care benefit programs, (b) fraud against patients, investors, and other non-governmental entities in the health care industry, where the overwhelming majority of the actual or intended loss was to patients, investors, and other non-governmental entities, and (c) any other federal violations involving conduct related to health care not covered by the Federal False Claims Act…"

Source: *U.S. Department of Justice, "Department of Justice Corporate Whistleblower Awards Pilot Program," August 1, 2024*

The Department has signaled its awareness of the tension between the CEP update and the new whistleblower program, crafting certain incentives and requirements in the latter accordingly. For instance, the program does not set forth a requirement that whistleblowers first alert a company's internal compliance department prior to blowing a whistle to the government; however, DOJ attempts to balance this misplaced incentive by increasing potential whistleblower awards in those instances where an attempt was made to notify the company first and, correspondingly, to decrease awards when whistleblowers bypass internal compliance. Much, then, is left to the discretion of DOJ in applying such factors, and many compliance professionals have concerns about how such a distinction works in the real world where time is of the essence in self-disclosing misconduct. Internal investigations and compliance procedures take time to execute; whistleblowers need only pick up a phone.

This leads to a second important source of tension between DOJ's CEP and new whistleblower program: declinations. A major incentive within the CEP is the notion that properly disclosed information will in many cases result in the government declining to prosecute, but the policy strongly suggests that declinations depend on the disclosure of new information. Whistleblowers, too, are on the clock, as the new program only awards those who volunteer information not already known. These policies create what is in effect a race to be first. Recognizing that this is less than ideal, DOJ has attempted to mitigate the negative aspects of the policy by creating a 120-day window during which a company can still qualify for a presumption of a declination after a whistleblower reports misconduct to the company and to DOJ.

The disclosure window notwithstanding, DOJ has stated explicitly that a company is "only eligible for the presumption of a declination…if it reports to the Department before the Department contacts the company." As a practical matter, then, the new whistleblower program does not really diminish a company's prior efforts to develop state-of-the-art processes

for internal reporting and intake; however, it might change the methodology employed in voluntary self-disclosure and declination analyses. If the process regarding how and when to escalate a matter is muddy, companies could run the risk of failing to timely disclose.

While the Department has pitched this as a program to fill enforcement gaps, there is much about it that is unique; both whistleblowers and compliance teams will need to carefully consider the implications. First, it is a product of DOJ's Criminal Division, and one imagines that it will be deployed to abet criminal prosecutions. Many of the government's existing whistleblower initiatives, such as the False Claims Act, are aimed at bringing civil lawsuits. This distinction carries with it serious questions of due process, as well as concerns in connection with whistleblower anonymity and confidentiality.

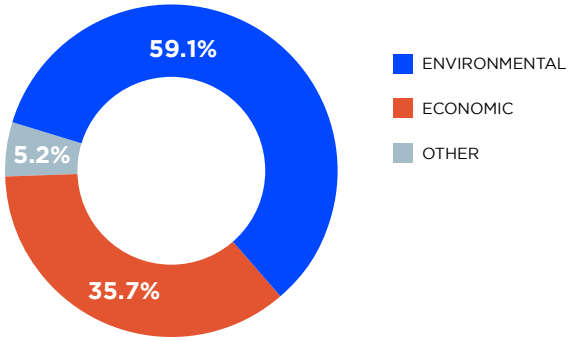
It also presents a couple of practical problems for the government of which corporate defendants should be aware. When the government is pursuing parallel proceedings with both criminal and civil components, the Criminal Division's whistleblower program could create challenges for interagency cooperation. The disclosure and dissemination of evidence collected in a criminal proceeding is guided by a very different set of rules than those in civil cases. Additionally, should the program wildly succeed, and the government lands a windfall of information regarding potential corporate malfeasance, there is still a necessity for the DOJ to sift and sort the information. The only thing worse than a lack of information is the inability to make use of information at hand. The former is a policy problem; the latter is a political problem and could backfire on the Department if information regarding a major corporate scandal was found to be sitting on a desk after the fact.

Supreme Court Seeks to Rebalance Federal Power

In a major development with broad implications for regulatory law, the October 2023 term of the U.S. Supreme Court featured two decisions that could recalibrate how federal agencies promulgate rules and enforce them. These decisions addressed very different questions of law, but taken together, they consistently signal the Court's desire to reallocate federal power away from the executive branch and administrative agencies and toward the legislature and judiciary.

The first of the decisions—*Securities and Exchange Commission v. Jarkesy*—ruled on the question of whether the U.S. Securities and Exchange Commission could employ its own in-house venue when seeking civil penalties against a defendant. Ultimately, the Supreme Court ruled that such a practice violated the Seventh Amendment's right to a jury trial and remanded the case to be tried again on that basis. It is expected that *Jarkesy* will have implications for numerous federal administrative agencies that use in-house venues to impose civil penalties. In her dissent, Justice Sonia Sotomayor listed several such agencies—including the Environmental Protection Agency (EPA)—whose ability to enforce civil penalties could be greatly impacted by *Jarkesy*. Given the costs associated with environmental law compliance for the manufacturing industry, compliance

DISTRIBUTION OF COMPLIANCE COSTS U.S. MANUFACTURING INDUSTRY



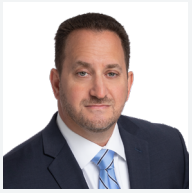
Source: *Nicole V. Crain and W. Mark Crain, "The Cost of Federal Regulation to the U.S. Economy, Manufacturing and Small Business: A Study Conducted for the National Association of Manufacturers," October 2023.*

teams should pay close attention to how EPA adapts to a post-*Jarkesy* world, both in terms of the enforcement actions it brings and the remedies sought.

Following closely on *Jarkesy*, the Supreme Court then decided *Loper Bright Enterprises v. Raimondo*, which involved arguments that struck at the heart of the so-called *Chevron* deference doctrine. For nearly 40 years, *Chevron*—named after a 1984 Supreme Court case upholding a Reagan-era EPA rule—required federal courts to defer to administrative agencies' interpretations of ambiguous statutes whenever

the agencies' interpretations are reasonable or permissible. The Court unambiguously ended this practice in *Loper Bright*, determining that *Chevron* deference cannot be squared with the Administrative Procedure Act (APA), which requires that courts reviewing agency actions "decide all relevant questions of law."

One of the main complaints with *Chevron* over the years has been the wildly vacillating nature of regulatory law from administration to administration, making compliance more costly and complex than it needs to be. It is believed that, by relocating the adjudication of "questions of law" to the judiciary, *Loper Bright* might bring greater certainty to the law, but that remains to be seen, as does whether such certainty is desirable. After all, some agencies have done commendable jobs in some areas of law, and not all heavily regulated industries may welcome the decision. Business-friendly agency rules and decisions will receive the same neutral adjudication on questions of law, and not all judges view administrative law as do the six justices of the Supreme Court who formed the majority in *Loper Bright*.



Gregg N. Sofer

is a partner in Husch Blackwell's White Collar, Internal Investigations & Compliance team and is based in Austin, Texas. Prior to entering private practice, he served as the United States Attorney for the Western District of Texas, as well as in high-ranking roles within the Department of Justice in Washington.

Rebecca Furdek

is a senior associate based in Husch Blackwell's Milwaukee, Wisconsin, office and a member of the firm's White Collar, Internal Investigations & Compliance team. Prior to joining the firm, she served as Counsel to the Solicitor at the U.S. Department of Labor.

Labor & Employment

ANNE MAYETTE AND TERRY POTTER

Employment-related issues continue to rate among the greatest concerns for manufacturers, who are under pressure to maintain high-functioning workforces while complying with an ever-larger body of law that regulates the workplace.

Before a gathering of organized labor and government officials at the White House in September 2021, President Joseph Biden **reiterated an intention** that he had stated many times before: "I intend to be the most pro-union president leading the most pro-union administration in American history." On several scores he remained true to his aim, much to the chagrin of private businesses that are struggling to keep up with the labor-friendly policies implemented by the administration.

Perhaps no area of public policy and regulatory enforcement has been more exposed to regulatory whiplash—that is, swift policy U-turns from one administration to the next—than labor and employment. From novel interpretations of workplace safety to the expansion of the National Labor Relations Act's "protected concerted activity," the Biden administration has stridently advocated pro-labor positions, any of which could be subject to reversal under a new administration or by the courts.

Workplace Safety

Workplace safety has always been an intensely regulated area of employment law with particular relevance to manufacturers, and 2024 was no different. The Occupational Safety and Health Administration (OSHA) continued to propose and finalize rules that add significantly to the cost of compliance or otherwise complicate once-settled processes and procedures.

One of the highest-profile actions was the agency's so-called Walkaround Rule, which empowers employees to appoint individuals they deem fit to represent them during an inspection. This may be another worker or, notably, a non-employee. The new rule adds language that greatly expands third parties who might gain access to workplaces under the reasonable necessity standard, including those who possess "language or communication skills" deemed relevant by the OSHA inspector. Additionally, OSHA's inspectors will "have authority to resolve all disputes as to who is the representative authorized by the employer and employees for the purpose of this section," which potentially removes administrative due-process constraints with which employers could contest OSHA's judgment regarding non-employee representatives.

The rule is controversial in that it could provide a side door for union organizers to gain access to non-union workplaces. It has also been noted that the rule could provide the plaintiffs' bar with valuable insights to use in litigation against employers more generally. For these reasons and myriad others, the rule was targeted by industry and trade groups even before its effective date, with perhaps the most high-profile of these efforts being a federal lawsuit in Texas filed by the U.S. Chamber of Commerce, the National Association of Manufacturers, and Associated Builders and Contractors, Inc., among other plaintiffs.

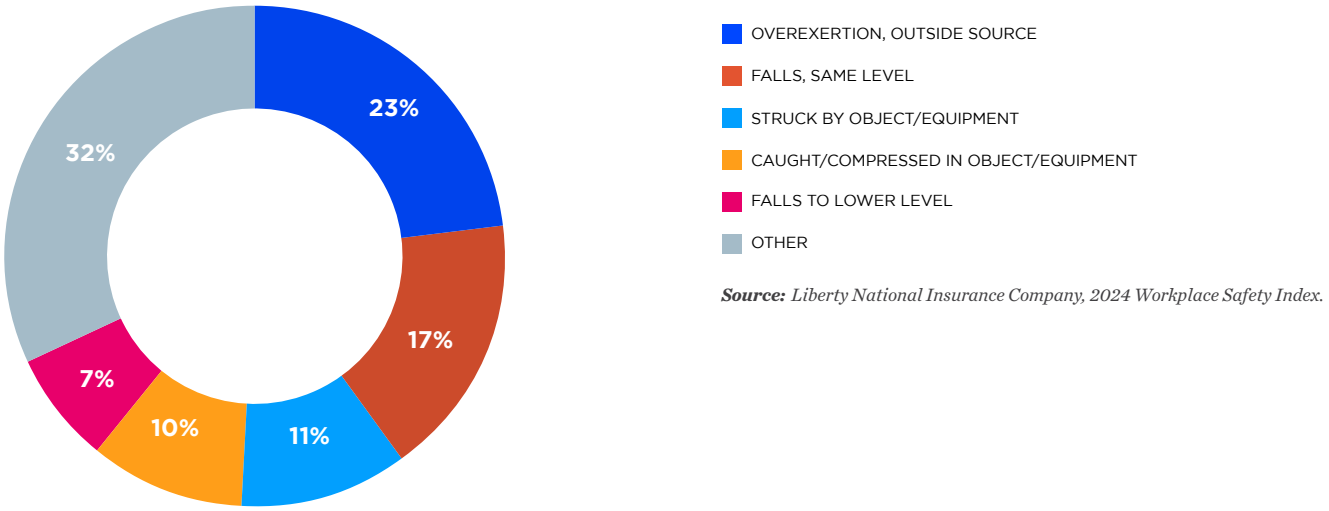
In addition to the Walkaround Rule, OSHA pushed forward new workplace safety rules in 2024 that more directly impact current compliance efforts. In January, its final rule requiring new submissions of injury and illness data for certain employers in high-hazard industries took effect. The rule will require certain employers to electronically submit injury and illness information they must already maintain to OSHA directly. OSHA indicated in its press release that it intends to publish some of the data it collects from these submissions on its website "to allow employers, employees, potential employees, employee representatives, current and potential customers, researchers and the general public to use information about a company's workplace safety and health record to make informed decisions." OSHA has also indicated that "it will use this data to intervene through strategic outreach and enforcement to reduce worker injuries and illnesses in high-hazard industries." The new rule requires covered establishments with 100 or more employees to electronically submit information from their Form 300 and Form 301 to OSHA once a year. This submission is in addition to the obligation to submit Form 300A.

52,000

Number of employers impacted by OSHA's new revised rule concerning occupational injury and illness recordkeeping.

MANUFACTURING INDUSTRY TOP LOSS CAUSES

The U.S. manufacturing industry lost $7.53 billion due to workplace-related injuries last year.



Source: *Liberty National Insurance Company, 2024 Workplace Safety Index.*

After hinting at it for years, OSHA announced in July 2024 a proposed rulemaking that would establish comprehensive requirements for employers to protect employees from heat-related injuries. The proposed rule would apply to many manufacturing enterprises, with exemptions for activities involving minimal heat exposure, indoor work areas or vehicles consistently kept below 80°F through air conditioning, and certain emergency response operations. Telework and sedentary indoor activities are also exempt.

OSHA'S PROPOSED "HEAT RULE": KEY REQUIREMENTS

HEAT INJURY AND ILLNESS PREVENTION PLAN (HIIPP)

Employers must develop a site-specific HIIPP that includes a list of covered work activities, policies to comply with the rule, and a method to identify heat conditions. The HIIPP must also designate a heat safety coordinator responsible for ensuring compliance.

HEAT TRIGGERS

Employers must monitor heat conditions using an approved heat metric to determine when certain requirements apply. There are two main triggers: the initial heat trigger and the high heat trigger. Generally, the initial heat trigger is at a heat index of 80°F, and the high heat trigger is at a heat index of 90°F.

INITIAL HEAT TRIGGER

When temperatures reach or exceed the initial heat trigger, employers must implement safety measures, such as providing cool drinking water and break areas either in the shade or in an air-conditioned space. Employers must encourage employees to take paid rest breaks if needed and effectively communicate with employees about the conditions.

HIGH HEAT TRIGGER

More rigorous safety measures apply when temperatures reach or exceed the high heat trigger. Employers must provide a minimum 15-minute paid rest break every two hours and notify employees about the importance of drinking water, their right to take rest breaks, and how to seek help in a heat emergency. Employers are also required to implement a preapproved method for observing employees for signs and symptoms of heat-related illness.

ACCLIMATIZATION, TRAINING, AND EMERGENCY RESPONSE

Employers must implement a preapproved protocol to help new and returning employees acclimatize to heat conditions. Annual training on safely working in the heat is required for all employees. Supervisors must also receive annual training on how to supervise employees working in conditions at or above the initial heat trigger. Additionally, employers must develop and implement a heat emergency response plan that aligns with the rule's requirements.

Wage & Hour Litigation Trends

Lawsuits filed in connection with the Fair Labor Standards Act (FLSA) have actually decreased over the past decade; however, settlement values have run conspicuously higher in recent years, topping an average of $1 million in 2023. Furthermore, the U.S. Department of Labor (DOL) has continued its audit and enforcement activity, bolstered by larger staffs and budgets. In 2023, DOL's Wage and Hour Division recovered over $274 million in back wages and damages from private businesses, most of it connected to overtime violations.

Overtime Exemptions

In April 2024, the DOL implemented its **final rule that raises the salary basis for overtime exemptions** under the FLSA. Because the rule necessarily increases employee compensation and sets in motion changes to exempt classification criteria, it immediately faced challenges in federal court. In July, the U.S. District Court for the Eastern District of Texas **granted an injunction** requested by the State of Texas, preventing the DOL from enforcing its rule.

The injunction's scope is narrow; it applies only to individuals employed directly by the State of Texas and does not include private employees in Texas or any other jurisdictions, but the reasoning in the opinion—which suggests that the DOL lacks the authority to issue this rule—will likely have an impact on the pending and future legal challenges regarding the DOL's ability to enforce the rules against employers more broadly. Manufacturers should follow the overtime rule's status closely and be prepared to comply with it should court challenges fail. The two-step increase for the standard salary level requirement for executive, administrative, professional, and computer employees, if it stands, is substantial, with 2025 levels representing a 65 percent increase from the pre-rule level.

Independent Contractors

Traditionally, manufacturers have not relied heavily on independent contractors, but those who do should pay close attention to a DOL **final rule issued in January 2024** that changes the methodology for determining whether a worker is an "employee" subject to FLSA or an independent contractor. This rule rescinds a Trump-era rule from 2021 and returns to a flexible "totality-of-circumstances" test to assess economic reality. The final rule took effect on March 11, 2024.

Just as DOL's withdrawal of the 2021 rule occasioned lawsuits from private businesses, the new rule was immediately targeted for litigation, and the fate of the rule remains in doubt.

PAGA Reform

In a rare bit of good news on the wage-and-hour front—at least, if you have operations in California—in June 2024, California Governor Gavin Newsom, alongside business and legislative leaders, **announced a significant agreement** to reform the state's Labor Code Private Attorneys General Act of 2004 (PAGA), which allows employees to bring enforcement actions against their employers on behalf of the state for alleged violations of the California Labor Code and provides employees with a 25 percent cut of the penalties assessed. As one might imagine, PAGA has been subject to abuse, including the extraction of large settlements from employers for technical violations that did not cause any actual damage to an employee.

While the reforms do not remove PAGA as a source of worry for California-based manufacturers, they do allow employers to significantly reduce penalties if they take "all reasonable steps" to comply with the Labor Code, either before or within 60 days of receiving a PAGA notice. Thus, the cure provisions will likely become a significant part of responding to PAGA actions given the potential for substantial reductions in penalties.

Anne Mayette

is Chicago-based partner in Husch Blackwell's Labor & Employment practice with deep experience both in house and in private practice assisting manufacturing and technology companies with workforce-related challenges.

Terry Potter

is senior counsel in Husch Blackwell's St. Louis office and its Labor & Employment practice and is a former field attorney with the National Labor Relations Board.

Artificial Intelligence

DUSTIN TAYLOR

As the hype subsides, the real work of integrating generative artificial intelligence into day-to-day operations has begun, and manufacturers are well placed to take advantage across all facets of operations, from design and production to supply-chain optimization.

Manufacturers have been using artificial intelligence (AI) in their operations for years, but recent advances in generative AI—that is, AI that creates new content by learning patterns from existing data—have expanded the scope of what is possible. As use cases proliferate, so, too, do the risks associated with AI, especially as federal, state, and local governments begin crafting regulations to manage its use.

UNDERSTANDING THE VARIETIES OF AI

ARTIFICIAL INTELLIGENCE
A broad term encompassing the development and use of computer systems capable of performing tasks that typically require human intelligence.

MACHINE LEARNING
A subset of AI that trains systems to learn from data and make decisions or predictions based on patterns.

NEURAL NETWORKS
A type of machine learning algorithm that mimics the structure and function of the human brain—allowing AI systems to learn and process complex data.

DEEP LEARNING
A subfield of machine learning that uses neural networks with multiple layers to learn and extract features from data.

GENERATIVE AI
A subset of AI that focuses on generating new content, such as text or images, based on patterns learned from data.

Source: *Gabriela Jhean, "AI vs Generative AI: What's the Difference?" May 21, 2024*

Because AI is a broad umbrella term and different forms of AI use data in different ways, it is important to precisely define AI when performing legal or regulatory risk assessments. At their core, traditional forms of AI and generative AI are similar. In implementation and scope, however, they are very different. For example, traditional AI may be trained on millions of users' video-watching history to suggest what a specific user may like to watch next. Generative AI is trained on hundreds of millions (or even billions) of wide-ranging media to suggest (or generate) new content. Whereas traditional AI may be used to make suggestions among thousands or even millions of possibilities, generative AI is being used to create new content. In the manufacturing setting, that could be new design options that calculate a complexity of factors, such as weight, strength, or specific materials, or production-related tasks.

Intellectual Property and AI

The earliest and most compelling applications of generative AI to manufacturing have involved core operations related to design and production, including rapid prototyping, autonomous operations, and predictive maintenance. As such, cutting-edge legal considerations for manufacturers often touch upon intellectual property (IP), especially given that IP law generally does not protect ideas themselves, but rather the way in which ideas are implemented or take shape. Furthermore, if something is well-known and deemed to belong to the public at large, IP law will not protect it, so as more companies and individuals begin using generative AI, their use creates numerous risks—both to IP that already exists and to the ability to claim new IP.

Manufacturers concerned about the risks presented by generative AI can take several steps to reduce those risks. First, adopt an AI policy that sets out clear guidelines on how AI can (and cannot) be used at your company. The policy should focus not only on what tasks can use generative AI (the output), but what information can be used to accomplish those tasks (the input). Second, perform an audit to determine to what extent your company is potentially disclosing proprietary information to open-source resources, such as GitHub. Third, keep up to date on changing laws that may affect your IP rights. AI's legal and regulatory setting is evolving on an almost daily basis. Finally, create a framework to help you make educated decisions about when it is okay to use new forms of AI (and when it makes sense to consult an outside expert for more information). AI is a rapidly changing area of technology and manufacturers need a framework in place that balances their company's priorities and risk management while allowing the company to use new forms of AI.

AI vendor contracts should also address IP considerations. Every contract should address IP ownership between the parties, including ownership of not only what the manufacturer inputs into the AI solution, but what the solution outputs as well. Because the output may be based on vast amounts of data on which the AI solution trained, the answer to this latter question may be more difficult. If a company provides inputs or prompts to the AI product/service, then the company will likely want to maintain its ownership rights over that input or prompt. Additionally, if a company's inputs or prompts are used by the AI product/service to create any output, then the company will likely want ownership rights over any output, including any work product or deliverable created from that output. The company should consider at least prohibiting the use of that output from being used for other purposes, including additional training of the AI.

Another ownership consideration is whether the AI vendor's product or service relies on a third party's technology. Many vendors are relying on third-party technology for their own AI models. Companies should require vendors to represent and warrant that the vendor has the right to use the third party's technology through a license and shall comply with all use restrictions under that license. Any representation and warranty should also make it clear that the vendor has full power and authority to grant the rights under the contract to the company.

Finally, for all AI products/services, vendors should also represent and warrant that the products/services will not misappropriate, violate, or infringe any third-party IP rights. Companies should consider indemnification protection for any claims that result from the misappropriation, violation, or infringement of any third-party IP rights and corresponding liability for any indemnification obligation.

ASSESSING AI RISK BY INTELLECTUAL PROPERTY TYPE: A PRIMER

COPYRIGHTS

- Website copy/image can be protected by copyright if human-created, but not if Gen-AI creates the content.
- Use of Gen-AI can expose a company or individual to claims of copyright infringement.
  - Cases filed to date mostly allege infringement by copyright owners naming the companies who design and program the Gen-AI tools, rather than the end users.
  - Companies that have custom-trained Gen-AI tools could find themselves named as defendants in lawsuits if they use copyrighted material to train those tools.

TRADE SECRETS

- Trade secret definition includes "all forms and types of…business…information" so long as "the owner thereof has taken reasonable measure to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means…"
- Information is significantly less likely to be considered a trade secret when created in whole or in part by Gen-AI.
- If trade secret information is publicly disclosed when used to train Gen-AI, the information will likely be deemed to no longer meet the trade secret definition.

PATENTS

- Assume something generated by Gen -AI technology cannot be protected by patent.
- Although the USPTO has not completely foreclosed the ability to obtain a patent if the inventor use Gen-AI during the invention process, it did reiterate the restrictions that only a natural person can be deemed an inventor.
- Unlike copyright, AI IP lawsuits have not (yet) alleged patent infringement.

TRADEMARKS

- Trademark law has to date been the least affected by Gen-AI.
- Trademark law does not require the word- or design-mark to have been created by a human to receive protection.
- Because Gen-AI tools are trained on existing material, there is a significant risk that any logo or design is confusingly similar to an existing trademark. Use of Gen-AI to create marks which are then used to offer goods and services can present risk of trademark litigation.

Striking Deals Involving AI

When manufacturers opt to utilize third-party AI tools and services rather than attempt to develop those tools internally, it is important to develop a standard process for onboarding the vendor and perform a risk assessment for the technology. As a starting point, companies need to identify key information such as the specific use case and business reason for using the product, the product/service's inputs and outputs, whether the product is being used for a high-risk processing activity, and the vendor's access to company data. If the vendor insists on using its contractual terms, the analysis also should identify whether those terms are negotiable and, if not, whether the company is willing to assume the risk of whatever terms are presented. If the vendor is a start-up, will the company be left holding the bag if the vendor closes shop in the face of third-party litigation, regulatory investigations, or business failure?

Although specific terms will depend on the exact use case, terms that typically require definitions are artificial intelligence (or a similar term like AI technology), generative AI, inputs, and outputs. Defining artificial intelligence is particularly important given that it establishes the scope of all obligations.

"Third-party offerings" is another common and significant term if the vendor's product/service will be used in combination with a different vendor's product/service. As touched on above, this is a common occurrence as many AI products/services are built on another vendor's product/service such as OpenAI. The underlying vendor's terms may alter or nullify any warranties or indemnification provisions and, therefore, require close review.

In addition to defining the key terms, contracts should address obligations and rights regarding inputs (i.e., what information goes into the AI) and outputs (i.e., what information comes out of the AI). With respect to inputs, companies need to consider what data will be provided, whether it will be secured by the vendor, and whether privacy or business proprietary considerations come into play. For example, if the company will input customer data, the contract should address privacy considerations and a data processing agreement may be appropriate. If the company will input business proprietary information, the contract should require the vendor to keep that information confidential and use it only for the company's business purposes. The contract also should address how the vendor can use and share the data, including whether it can use the data to improve or train its product.

Relatedly, depending on the scope of the data shared with vendors, companies should consider adding data breach notification and defense/indemnity clauses if they are not already addressed in the contract or data processing agreement. It is not difficult to imagine that these AI products and services will be a new threat vector for hackers.

For outputs, the contract should address which contracting entity owns the outputs. For example, some AI vendors are now specifically acknowledging ownership issues regarding outputs in contractual agreements and ancillary materials. Most notably, Microsoft recently updated its consumer Services Agreement to expand "the definition of 'Your Content' to include content that is generated by your use of our AI services." In other words, Microsoft recognizes that the user—and not Microsoft—owns the output. For many manufacturers using third-party technology to design products or production processes, output-specific provisions will require careful scrutiny in order to secure ownership of the relevant intellectual property.

Dustin Taylor

is a Denver-based partner in Husch Blackwell's Technology, Manufacturing and Transportation industry group. He represents clients in intellectual property, artificial intelligence, computer access, and data privacy litigation.

Cybersecurity

ERIK DULLEA

As cyber threats increase and attack surfaces proliferate, protecting an organization's network systems, customer data, proprietary information, and operational technology against unauthorized access grows more challenging.

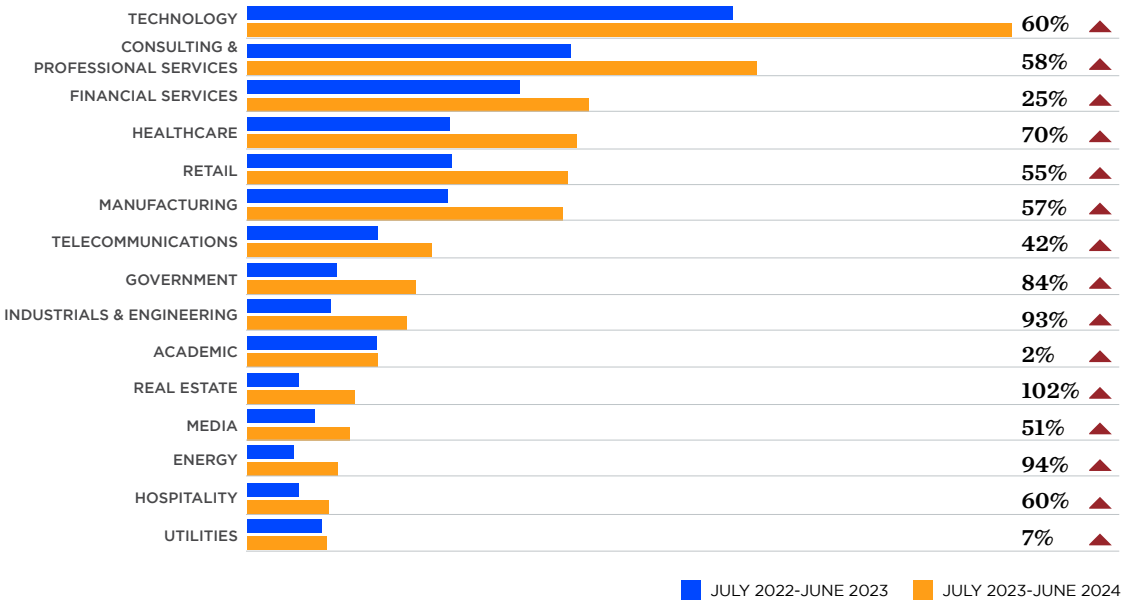
Cybercrime continues to be a booming market for criminals—and a growing challenge for information security professionals. According to an April 2024 report by the Congressional Research Service, cybercrime cost the United States an estimated $220 billion in 2022 and $320 billion in 2023. The expected costs in 2024 are $452 billion and are forecasted to exceed $1 trillion in 2027.

Cybersecurity, Manufacturing & Its Enabling Technologies

Consistent with last year's statistical trends, manufacturing remains a frequently targeted sector for malicious cyber activities. According to CrowdStrike, a cybersecurity company and provider of endpoint security services, the industry experienced a **57 percent increase in cyber intrusions** compared to the prior year, but what is equally concerning is the prevalence of attacks against the technology sector, which includes developers of software and hardware, information technology (IT), and IT service providers. These businesses are relied upon by every other industry sector—including manufacturing; therefore, the growing cybersecurity challenge for tech companies creates significant third-party risk.

Ironically, CrowdStrike provided a glaring case study on the ripple effects caused by a disruption within a technology services company. On July 19, 2024, the company was the

TOP SECTORS BY INTRUSION FREQUENCY



Source: *CrowdStrike 2024 Threat Hunting Report.*

source of a flawed software update deployed worldwide to Microsoft Windows servers, causing the "blue screen of death" across 8.5 million computers worldwide. Fortunately, the flaw was due to benign human error, not a malicious actor who sought to evade detection. Nevertheless, downstream consequences from a simple coding error in a software update illustrates both the liability risks manufacturers face when they place their electronic components into the marketplace, as well as the business interruption risk they face when receiving new components from their suppliers. Both require the attention of compliance, legal, and/or contracting teams to have plans in place in the event of a mishap.

CISA's Proposed Rules for Cyber Incident Reporting for Critical Infrastructure

In March 2024 the Cybersecurity and Infrastructure Security Agency (CISA) released a Notice of Proposed Rulemaking (NPRM) to implement regulations mandated by Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The proposed regulations echo Congress's statutory deadlines for large critical infrastructure companies to report substantial cyber incidents to CISA within 72 hours. Additionally, the law requires covered entities to report ransom payments to CISA within 24 hours of the payment being made.

While CIRCIA set forth these reporting timeframes, the statute did not expressly define covered entities or covered cyber incidents. The proposed regulations provide definitions for those terms. CISA's proposed definition for covered entities would be owners and operators of critical infrastructure that exceed the small business size standard associated with the owner/operator's North American Industry Classification Standard, or NAICS, code. CISA's proposed definition for a covered cyber incident would be a substantial cyber incident experienced by a covered entity.

Pursuant to the Patriot Act and two presidential directives, U.S. critical infrastructure is defined as those industry sectors with vital assets, systems, and networks (physical or virtual) such that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The Department of Homeland Security designated 16 industry sectors as critical infrastructure, each of which has an assigned Sector Risk Management Agency (SRMA) that is charged with providing resources and coordination to assist industry participants in the event of an incident.

CISA's proposed rule provides the **agency's methodology** for determining when a cyber incident is elevated to the category of *substantial cyber incident*, which is defined as an incident that leads to one of the following impacts:

- Substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- Serious impact on the safety and resilience of a covered entity's operational systems and processes;
- Disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or
- Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either (1) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (2) a supply chain compromise.

The proposed definition of a substantial cyber incident would require one or more actual impacts to occur. An attempt to cause a loss of confidentiality or disrupt a covered entity's ability engage in business would not be reportable because there was no impact.

SEC Cybersecurity Rule Developments

One concern that private industry has expressed with the increased cyber reporting requirements is that the information will be used by other enforcement agencies to punish the victim company. While there is always a risk of dubious enforcement actions in the absence of safe harbor provisions within reporting laws, the SEC's efforts to become a cybersecurity enforcement agency—discussed at length in last year's report—hit a roadblock this summer in the SEC's case against SolarWinds.

On October 30, 2023, the SEC filed a complaint against SolarWinds, a software development company, and its chief information security officer (CISO). The complaint caused significant concern among the information security community

DESIGNATED SRMA BY INDUSTRY SECTOR

Sector	DHS	DOD	DOE	DOT	EPA	GSA	HHS	TREAS	USDA
CHEMICAL	●								
COMMERCIAL FACILITIES	●								
COMMUNICATIONS	●								
CRITICAL MANUFACTURING	●								
DAMS	●								
DEFENSE INDUSTRIAL BASE		●							
EMERGENCY SERVICES	●								
ENERGY			●						
FINANCIAL SERVICES								●	
FOOD AND AGRICULTURE							●		●
GOVERNMENT FACILITIES	●					●			
HEALTHCARE/PUBLIC HEALTH							●		
INFORMATION TECHNOLOGY	●								
NUCLEAR	●								
TRANSPORTATION SYSTEMS	●			●					
WATER/WASTEWATER					●				

Source: Presidential Policy Directive—Critical Infrastructure Security and Resilience, February 12, 2013.

because the SEC alleged that between the date SolarWinds became a publicly traded company (2018) and January 2021, SolarWinds made materially misleading statements and omissions in public disclosures and statements regarding the company's cybersecurity practices. The SEC argued these statements caused a significant drop in the company's stock price after the December 2020 disclosure of a large-scale cybersecurity attack known as SUNBURST.

The statements that the SEC took issue with included the company's periodic filings that only described generic and hypothetical cybersecurity risks but failed to specify cybersecurity risks that were known to the company. The SEC argued that the SolarWinds online security statement claimed that the company followed cybersecurity standards like the National Institute of Standards and Technology Cybersecurity Framework, utilized strong authentication and password policies, and maintained adequate access controls when those practices were not followed. The SEC also alleged the company and CISO of concealing deficient cybersecurity controls and identified vulnerabilities that left its systems

KEY TAKEAWAYS FROM SOLARWINDS CASE

ALLEGATIONS DISMISSED		ALLEGATIONS NOT DISMISSED
SolarWinds and its CISO had engaged in securities fraud based on the CISO's public statements in podcasts, blog posts and press releases that stated SolarWinds adhered/was dedicated to high cybersecurity standards. *The court concluded those public statements were simply corporate puffery and were too general for a reasonable investor to rely on them.*	**SolarWinds had ineffective disclosure rules as required by Exchange Act Rule 13a-15(a).** *The court concluded that the SEC could not take enforcement action based on second-guessing with the benefit of hindsight, or simply because errors were made while utilizing the existing SolarWinds disclosure controls.*	**SolarWinds' security statement was fraudulent.** *False statements made on publicly accessible websites can support a securities fraud claim, and the court denied the defendants' motion to dismiss the claim that. The court compared the online security statement to the company's internal assessments, communications, and presentations discussing deficiencies in its cybersecurity program.*

susceptible to attack, which were highlighted by internal company records voicing concerns with the deficiencies.

Based on those facts, the SEC charged SolarWinds and its CISO with direct anti-fraud violations for alleged misstatements as well as direct and secondary liability against them for internal controls violations. The defendants moved to dismiss the complaint, which the court partially granted on July 18, 2024 (four days before the CrowdStrike patching error disrupted the world's economy for a few hours). The court's decision was significant because it addressed several concerns within the information security community regarding the SEC's enforcement powers over a company's cybersecurity practices.

Notably, the court compared the company's online security statement to its internal assessments, communications and presentations discussing deficiencies in its cybersecurity program. These internal assessments and communications are vital to a company's ability to identify, prioritize and assess its cybersecurity risks, and those communications should not be stifled.

However, corporate leaders must acknowledge that such assessments and communications can be used in enforcement actions if they are apposite to the company's official statements to customers and investors about its security controls. Accordingly, publicly traded companies—and those aspiring to be publicly traded or acquired—must strive to be consistent between their cybersecurity assessments and their public statements on cybersecurity.

Erik Dullea

is a Denver-based partner in Husch Blackwell's Technology, Manufacturing and Transportation industry group who formerly served as the acting deputy associate general counsel of the National Security Agency's cybersecurity practice group.

SPOTLIGHT ISSUE

PFAS

DOMINIQUE SAVINELLI

Between federal and state PFAS regulations, manufacturers face mounting pressures to address the use of PFAS throughout the supply chain.

As the regulatory landscape surrounding PFAS continues to develop, in the past year alone, the Environmental Protection Agency (EPA) has taken no fewer than seven new actions to address PFAS, and dozens of states continue to finalize new regulations of their own, often with greater restrictions. The many nuanced—and at times inconsistent—regulations strain the manufacturing industry as it navigates a compliance minefield.

Among the actions taken by the EPA this year, in April 2024, the agency finalized a rule to designate two widely used PFAS (Perflurooctanoic Acid, or PFOA, and Perfluorooctanesulfonic Acid, or PFOS) as hazardous substances under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA); issued a national, legally enforceable drinking water standard; eliminated the threshold for reporting certain PFAS compounds in Toxic Release Inventory reporting; and announced changes to the General Services Administration's custodial specifications to ensure that cleaning products purchased for federal buildings are free of "toxic PFAS." These new actions add to already burdensome rules imposed on manufacturers while they continue to gather data under the EPA's Toxic Substances Control Act (TSCA) Reporting and Recordkeeping Requirements for PFAS final rule.

The EPA's TSCA Rule went into effect in November 2023 with reporting deadlines extending into 2025. According to the EPA, it finalized this rule "both to fulfill its obligations under TSCA section 8(a)(7) . . . and to create a more comprehensive database of previously manufactured PFAS to improve the Agency's understanding of PFAS in commerce and to support actions to address PFAS exposure and contamination." Essentially, without an understanding of the extent to which PFAS is used nationwide, the EPA plans to use these extensive reporting requirements to gather broad information about PFAS' role in manufacturing, findings which will likely lead to additional regulations.

Initially, all entities that have manufactured or imported PFAS in any year since 2011 had 18 months following the effective date—November 13, 2023—to report the above data to the EPA; however, in September 2024 EPA **granted companies an eight-month extension**, citing "a budget shortfall that has delayed the agency's ability to develop a fully functioning reporting tool in time for its November start date." This decision moves the start date of the information submission period for most to July 11, 2025, which will end January 11, 2026. This amendment to the final rule also extends the reporting period for article importers that are small manufacturers (as defined by 40 C.F.R. 704.3) until July 11, 2026.

The rule requires that all manufacturers, including importers, determine which products they manufactured or imported for a commercial purpose contain PFAS, including all articles or component parts of said products. The term "manufacture" extends to "substances that are produced coincidentally during the manufacture, processing, use, or disposal of another substance," so there is no exemption for impurities. The standard for determining and reporting which products contain PFAS is "information known to or reasonably ascertainable by [the manufacturer]." "This standard carries with it an exercise of due diligence," and requires that reporting entities "conduct a reasonable inquiry within the full scope of their organization," as well as may "entail inquiries outside the organization" such as contacting "upstream suppliers or downstream users or employees or other agents of the manufacturer."

2023 TSCA RULE REPORTING & RECORDKEEPING REQS

Source: U.S. Environmental Protection Agency.

Accordingly, to be in compliance with the rule, the EPA requires any entity that manufactured or imported a product that contained PFAS at any point since 2011 to conduct its due diligence to ascertain which products or articles contained PFAS, even if the product was manufactured after 2011 but is no longer in circulation. To accomplish this, manufacturers and importers are not required to test products, but most likely will need to reach out to their suppliers, who likely will then need to reach out to their suppliers, and so on, to provide documentation indicating whether any article supplied contained PFAS. Under this rule, it will not be sufficient for, say, a chair manufacturer to report that no bulk PFAS was contained in the chair. The manufacturer will also need to make an effort to determine if any components of the articles, such as paint, vinyl, fabric, coating, screws, leather, etc., had PFAS in them at all.

The rule encourages entities that are not able to reasonably ascertain whether they manufactured or imported a product, or article, that contained PFAS at any time since 2011 to "document [their] activities to provide evidence of due diligence." The burden to the industry comes at no small cost: the EPA estimates that resultant costs to the industry by undertaking this process would be approximately 11.6 million hours and roughly $800 million; furthermore, the TSCA final rule is merely one initiative of many that is in play at the federal level.

Along with the TSCA Rule and the EPA's multiplying PFAS regulations, manufacturers also face heavy state-level legislation dictating PFAS use and limitations across multiple product types, including firefighting foam, drinking water, food packaging, textiles, and other consumer products. Although these regulations have different compliance timelines and reporting requirements, they commonly emphasize a ban on "intentionally added PFAS," largely in consumer products. For example, Maryland Senate Bill 273 prohibits—beginning January 2024—"the manufacture, sale, and distribution for sale or use" of products within the state that contain "intentionally added" PFAS, including new rugs or carpets, food packaging, and firefighting foam (with several temporary exceptions). A company that manufactures or sells rugs, carpets, or food packaging in Maryland—if requested by the state—may be required to provide a certificate of compliance to attest that the product is in compliance with the law, which also provides for civil penalties that may increase up to $1,000 per violation.

Colorado has a similar law, HB22-1345, that provides limitations beginning in January 2024, for carpets, rugs, fabric treatments, food packaging, juvenile products, and oil and gas products. This bill also requires that, if a manufacturer of cookware sells a product that contains intentionally added PFAS chemicals in the state, the product label must list the presence of PFAS chemicals and a statement that directs consumers to a website where they can find information about why PFAS chemicals were intentionally added. Likewise, Maine has a bill, H.P. 1113-L.D. 1503, that became effective in January 2023, which prohibits the sale or distribution by January 2030 of "any product that contains intentionally added PFAS," unless the state has determined that such use was "unavoidable." Like Maryland, Maine's law permits the state to require a certificate of compliance from the manufacturer if it suspects that a product contains intentionally added PFAS in violation of the law.

Navigating the ever-changing PFAS compliance landscape is burdensome, and unfortunately, it does not appear that either the federal or state governments' regulation of this area will let up anytime soon. Staying on top of reporting and other regulatory or legislative requirements, while costly, allows companies to avoid further government inquiries and possible civil penalties.

PFAS-RELATED FEDERAL ACTIONS, 2021-2024

2021

- Denial/Withdrawal of TSCA LVEs
- More Stringent Existing & New Chemical Manufacturing, Importation, and End-Use
- TSCA Reviews, Inventory Re-reviews, Rules, and Orders
- TSCA Section 4 Test Orders
- PFAS Categories Identification
- Final Toxicity Assessment for PFBS & Gen X
- Increased Enforcement/Oversight via RCRA, TSCA, CWA, SDWA, CERCLA
- Total Adsorbable Fluorine (TAD) Method for Wastewater

2022

- National Ambient Water Quality Criteria for Aquatic Life
- Health Advisories for PFBS & GenX
- Voluntary Stewardship Program for Industry
- Hazardous Air Pollutant Designation
- Expanded TRI Reporting/ Chemicals of Special Concern Designation
- Soil Leaching Analytical Method
- Multimidia Test Methods for 40 PFAS
- IRIA Assessments for PFBA, PFHxS, PFHxA, PFNA, PFDA
- Annual Progress Report on PFAS Strategic Roadmap
- Final ELG Plan 15
- National Fish Tissue Surveys
- Drinking Water Treatment Technologies

2023

- CERCLA Hazardous Substance Designation/Cost Recovery
- TSCA 2011 Retroactive Reporting
- UCMR 5 Implementation
- Additional Health Advisories
- NPDES Permitting
- Update Guidance on Destroying & Disposing PFAS
- Fish Consumption Advisory PFAS List

2024

- National Primary Drinking Water Regulations
- National Ambient Water Quality Criteria for Human Health
- Additional Health Advisories
- Effluent Limitation Guidelines
- Drinking Water Methods Updates
- Biosolids Risk Assessment

Source: Adapted and revised from ***Trihydro Corporation.***

Dominique Savinelli

is a partner based in Husch Blackwell's Link office and focuses on complex mass tort and class action litigation involving the chemical, agribusiness, and insurance industries.

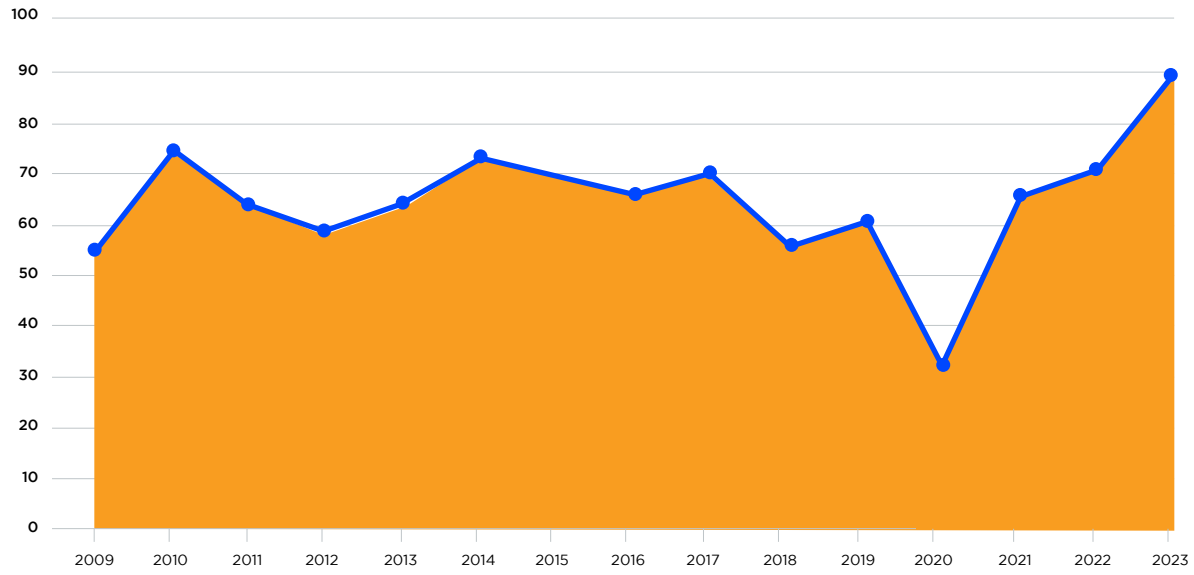
Product Liability, Safety & Marketing

BRANDAN MUELLER

Manufacturers are currently operating in an era of "nuclear verdicts" and unconventional regulatory enforcement tactics that contribute to a sense of unease and a growing risk profile.

In last year's report, we noted a post-pandemic trend of more filings in products-related cases and a higher level of sophistication from the plaintiffs' bar in pursuing litigation. These trends continue to exert influence and are now becoming evident in the form of so-called "nuclear verdicts," that is, jury verdicts that surpass $10 million in damages. In 2023, we reached a new high-water mark for such verdicts, continuing the post-Covid trend toward costlier damage awards.

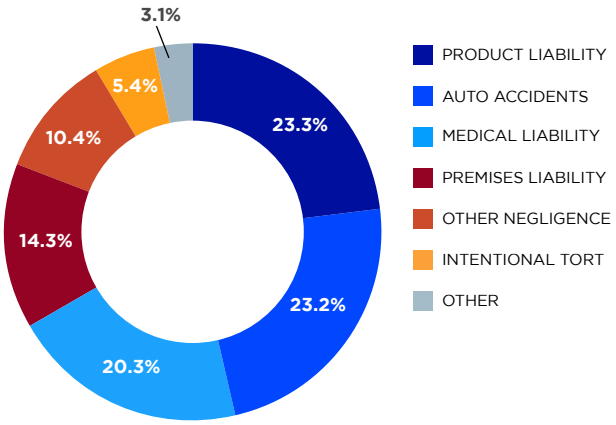
CORPORATE NUCLEAR VERDICTS, 2009-2023



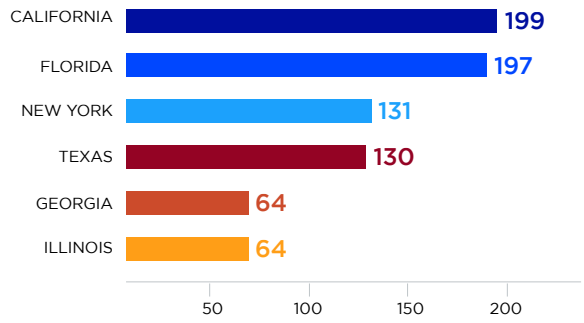
Source: *Marathon Strategies, Corporate Verdicts Go Thermonuclear (2024 edition).*

Clearly, the risks posed to product manufacturers by private litigation are broad-based and growing. Among the types of litigation that figure into these outsized jury verdicts last year, product liability ranks at the top of the list at 38 percent, according to Marathon Strategies, a communications and public relations consultancy. Similarly, according to the U.S. Chamber of Commerce, product liability nuclear verdicts are rising in size far more quickly than other verdict types, experiencing a 50 percent increase since 2013. There were over 50 industries that faced exposure to nuclear verdicts according to Marathon's research, including chemicals, automobiles, and home furnishings, to name a few in the manufacturing sector.

NUCLEAR VERDICTS BY TYPE AND LOCATION 2013-2022



TOP STATES BY CUMULATIVE NUCLEAR VERDICTS



Source: *U.S. Chamber of Commerce Institute of Legal Reform.*

Given that the threat of a nuclear verdict is far higher in state courts, venue is an important risk factor to consider; simply put, some states are more plaintiff-friendly than others. And that list could be growing. Maine, Delaware, Illinois, Minnesota, and Rhode Island each passed plaintiff-friendly laws that could encourage larger verdicts; by contrast, Florida has recently passed reforms likely to lead to a measurable drop in the damages associated with jury verdicts in the future, a notable development given that product liability has been the state's most frequent source of nuclear verdicts over the past decade.

A handful of other states—including Iowa, Indiana, Texas, West Virginia, Utah, and Wyoming—has passed or contemplated more modest legislation that could limit nuclear verdicts in those jurisdictions. These reforms typically address discrete elements of litigation that are prone to abuse, including third-party litigation funding disclosures, caps on noneconomic damages, and protections for specific industries (e.g. trucking and transportation) or against certain claims (e.g. asbestos-related).

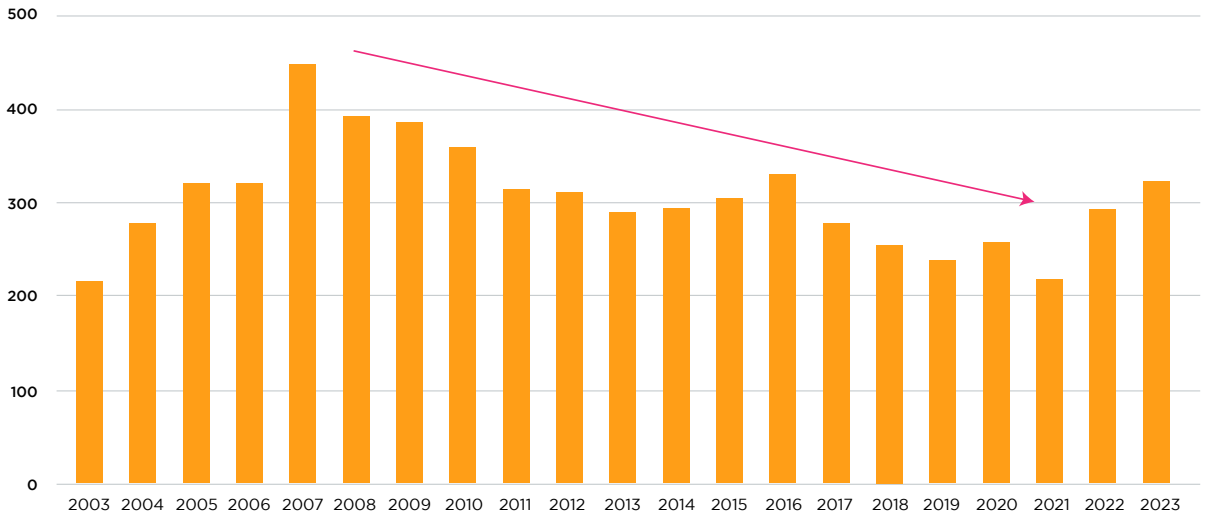
As seen above, state legislatures have taken very different approaches to legal reform. Manufacturers need to be aware of how key jurisdictions intersect with their operations and factor venue into their private litigation risk assessments.

Recalls and Unilateral Press Releases

Private litigation is not the only threat faced by manufacturers. Federal and state regulatory agencies are also actively ramping up enforcement—sometimes employing unconventional or novel approaches—in connection with perceived violations of the many laws that regulate the manufacture, distribution, sale, and marketing of products.

Product recalls remain a source of worry for manufacturers. According to Sedgwick, a brand consultancy and insurance technology firm, the total number of allegedly defective products across U.S. industries surged 96.4 percent in the second quarter of 2024. This follows on a trend of increasing recall events established in the first quarter of the year, which saw the overall number of recalls increase eight percent on a quarterly basis, reaching the highest total in a single quarter since the onset the COVID pandemic. Specifically, the Consumer Product Safety Commission (CPSC) instituted 92 recalls during the first quarter, a slight increase from the previous quarter and the previous year's trend. Since the onset of COVID, CPSC recalls have reversed a decade-long trend toward fewer recalls, and early 2024 data suggest the new trend is gathering momentum.

CPSC PRODUCT RECALLS, 2003-2023
The post-COVID period has reversed a decade-long trend line of declining recalls.



Source: *U.S. Consumer Products Safety Commission.*

Perhaps as concerning as the rise of CPSC's use of formal recalls is its increasing reliance on so-called unilateral press releases. These are press releases issued by CPSC advising consumers to stop the use of certain products without the agreement of the manufacturer. The Commission has dramatically expanded its use of these releases. From 2011 to 2019, CPSC issued two such press releases. According to the Commission, it issued 26 unilateral warnings in 2023—that's more than the last five years combined.

When CPSC elects to forego the procedures of a formal recall, it places manufacturers in a uniquely vulnerable position where traditional due-process constraints are absent. Manufacturers will need to consider carefully how to engage with the CPSC when questions arise concerning alleged product defects and hazards in light of this regulatory approach. When a product is unambiguously hazardous to consumers or if a recall makes strategic sense when considering all factors, making use of CPSC's fast-track recall process and providing full cooperation can help manufacturers quickly overcome product-related challenges. In FY 2023, CPSC staff completed 313 voluntary recalls, and 167 of those were completed under the fast-track program; however, when an alleged product defect or hazard is a matter of dispute between a private business and the Commission, manufacturers need to be alert to the full range of actions available to CPSC, including unilateral press releases.

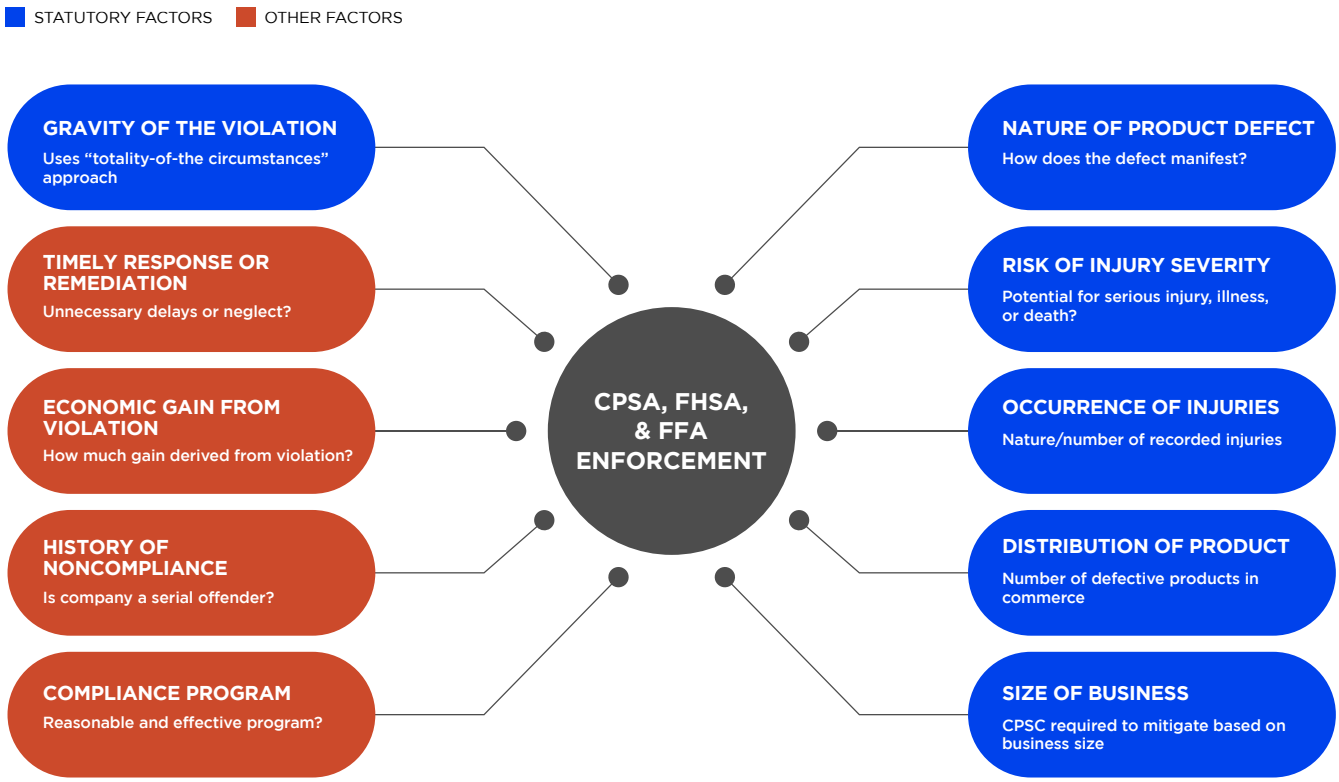
Regulatory Compliance and Risk Management

The trends touched on above do not alter the basic parameters for compliance teams engaged with the challenges posed by product safety and marketing. Disclosure requirements are front and center, and CPSC has signaled its intent to aggressively pursue civil penalties for noncompliance in

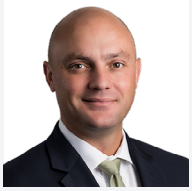
accordance with the statutory, regulatory, and sub-regulatory factors it has set forth in prior guidance. Since the beginning of 2022, those penalties total $120,000 for each violation and $17,150,000 for any related series of violations.

At times regulatory authorities and manufacturers disagree over what is "reasonable," which is often the legal standard for the variables at play in regulatory compliance. When those disputes arise, having an effective compliance program is invaluable, as it allows a business to defend itself when regulators overreach, and when product defects are uncovered, it allows businesses to mitigate civil penalties. But perhaps more importantly, a strong compliance program, which includes a robust employee training program and investigation procedures, can alert companies to problems before they emerge into public view. Being the subject of a government enforcement action is bad; getting hit with a thermonuclear verdict in private litigation—along with the associated destruction of brand value—can be far, far worse.

WHAT DOES CPSC CONSIDER IN DETERMINING CIVIL PENALTIES?



Source: *U.S. Code of Federal Regulations § 1119.4.*



Brandan Mueller

is a partner based in Husch Blackwell's Link office and the firm's Technology, Manufacturing and Transportation industry group. He routinely assists clients with the development of new products, product recalls, and litigation involving product liability and safety issues.

International Trade

CORTNEY MORGAN AND DAN WILSON

November's U.S. presidential election will play a significant role in determining the trajectory of trade policy; however, there are also larger trends at work that will likely transcend the election and persist well into the future.

The global economy continues to be buffeted by geopolitical tensions and the divergent strategic interests of major countries. Trade policy has emerged as a primary tool in responding to the changes that are reconfiguring foreign affairs, placing pressure on U.S. manufacturers to comply with an ever-expanding list of sanctions, duties, and restrictions on the crossborder flow of goods, services, and capital.

Countervailing Duties, U.S. Manufacturers and Evasion

One conspicuous example of how geopolitical changes outside the U.S. are impacting U.S. trade policy is the People's Republic of China (PRC) Belt & Road Initiative (BRI), under which the PRC has invested over $1 trillion to create a web of economic and logistical dependencies encompassing over 150 countries. The BRI was specifically cited by the U.S. Department of Commerce as one of its key areas of concern when it recently reconsidered longstanding policy not to consider so-called "cross-border" subsidies by modifying its regulations to claim the authority to investigate subsidies provided by third-country governments to manufacturers in countries under investigation. The modified regulations are generally applicable but are largely in response to increased Chinese foreign direct investment in other countries, including through the BRI.

Commerce previously limited its examination of subsidies to those programs and benefits provided by the investigated country to exporters within that investigated country. Formerly, a subsidy provided by the investigated government to the investigated company would be countervailable if it provided a financial contribution from the government to a producer and/or exporters that was specific, in that it provided the company, a group of companies, or an industry an unfair advantage to enable it to produce, and consequently export, more goods.

Commerce's amended regulations, among other things, claim statutory authority to examine "transnational subsidies," which casts serious uncertainty as to what constitutes a "countervailable" subsidy, as the regulations lack procedural and other specific factual guidance on how these third-party government subsidies will be examined and addressed as part of investigations and reviews. The new rules went into effect on April 24, 2024.

There is significant uncertainty around the government's new definition of specificity, making compliance efforts

considerably more difficult in the short run, particularly those concerning what subsidies to examine and report. It also provides Commerce more opportunities to make assumptions based upon adverse inferences when responding companies attempt to report programs and benefits received.

The new rules also have implications for the conduct of parallel antidumping duty proceedings in that the receipt of subsidies for raw material inputs could lead to an increased use of Commerce's unique "particular market situation" (PMS) analysis and further increase the burden on responding companies in reporting sales and production costs to the agency.

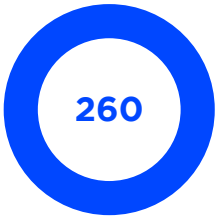
For U.S. manufacturers at large, countervailing duties can be something of a double-edged sword, aiding manufacturers when it levels the playing field vis-à-vis competing foreign products, but also potentially raising the costs of inputs used by domestic businesses. Perhaps no area of trade policy illustrates this as starkly as enforcement actions in connection with the Enforce and Protect Act (EAPA), which provides U.S.-based companies with a powerful tool to uncover and report the existence of allegedly transshipped goods in the U.S. marketplace. EAPA provides additional tools for U.S. Customs and Border Protection (CBP) to investigate importers that may not be paying duties at the time of entry. One key feature of the law is a provision allowing U.S. domestic producers to file allegations against importers suspected of evasion, in effect, turning private businesses into whistleblowers regarding "suspicious" products, many of which may compete with their own products. Like other legal frameworks that employ whistleblowers, EAPA can be highly effective at rooting out illegal behavior, but it can also lead to unfounded allegations that are shrouded in administrative secrecy, making it difficult for accused importers to mount a defense.

This circumstance can lead to legitimate due process concerns, an issue recently taken up by the Federal Circuit in *Royal Brush Manufacturing v. U.S. et al.*, which held that CBP violates importers' due process rights when it denies access to confidential information used against them in EAPA determinations. As a result, CBP announced in May 2024 that it will now issue administrative protective orders (APOs) granting accused parties access to business confidential information in EAPA investigations.

Section 301 Tariff Increases

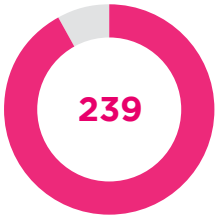
On September 13, the U.S. Trade Representative (USTR) released a **list** of significant Section 301 tariff increases that is largely consistent with a proposed **list** announced on May 22, 2024. USTR also announced an exclusion process by which U.S. manufacturers may request that "particular machinery used in domestic manufacturing be temporarily excluded from Section 301 tariffs." Finally, USTR included a limited number of temporary exclusions for certain manufacturing equipment. The specific products are identified by the U.S. Harmonized Tariff schedule code in the relevant annexes to USTR's September 13 notice.

EAPA BY THE NUMBERS



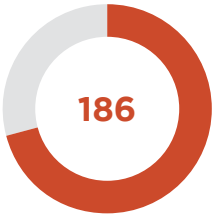
TOTAL INVESTIGATIONS

Investigations that have made it to the interim measures and/or determination stages of an investigation since 2016.



TRANSSHIPMENT

Investigations involving transshipments as the primary evasion tactic.



CHINA

Cases where the People's Republic of China is believed to be the possible country of origin.

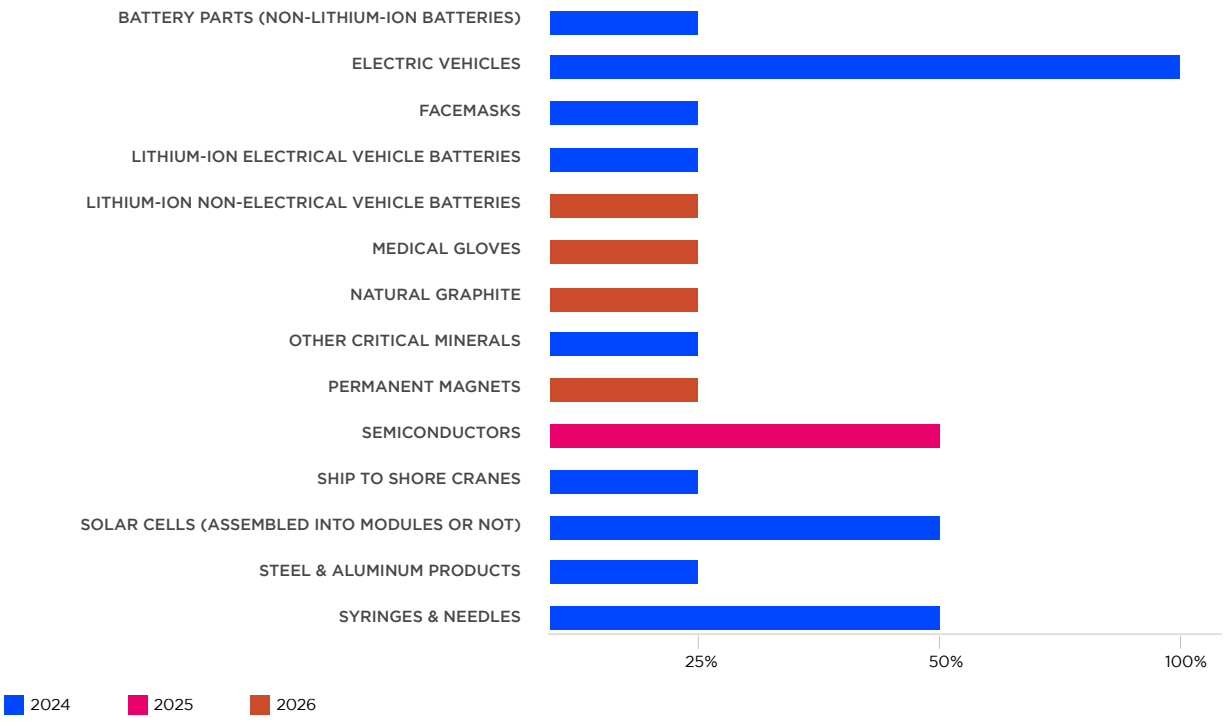
Source: *U.S. Customs and Border Protection. Updated May 8, 2024.*

USTR's increased Section 301 tariffs claims to target "certain products from China in strategic sectors," including lithium-ion batteries, electronic vehicles, solar power, steel, and aluminum, semiconductors, medical equipment and shipping. These industries have long been at the heart of the Biden administration's efforts at supply chain diversification and bolstering U.S. manufacturing. USTR has confirmed that the proposed tariff increases in these sectors include "products targeted by China for dominance or are products in sectors where the United States has recently made significant investments."

The tariff increases were foreshadowed by the publication of a USTR report detailing the results of its four-year review of the existing Section 301 measures. As expected, the report found that the Section 301 tariffs imposed during the Trump administration have had some positive effect in shifting U.S. supply chains away from China; however, the report also found ample opportunity to incentivize China to make further reforms in order to remedy the acts, policies, and practices related to technology transfer, intellectual property, and innovation found to have provided the basis for USTR to impose the Section 301 measures.

As mentioned above, USTR has proposed limited exclusions solely for imported equipment dedicated to U.S. manufacturing activity. Unlike prior rounds of Section 301 exclusions—where the question of domestic availability was at issue—the most recent round of exclusions are clearly aimed at incentivizing U.S. manufacturing and shifting supply chains away from China through alternative import sourcing. The USTR report noted that the 429 existing product-specific Section 301 exclusions were set to expire on May 31, 2024, and while the report hinted that a renewal of those exclusions was unlikely, USTR subsequently **elected to extend certain exclusions** through May 31, 2025.

PROPOSED SECTION 301 TARIFF INCREASES, MAY 2024



Source: *Office of the United States Trade Representative.*

Export Controls & Trade Sanctions Developments

Transshipment risks are significant for importers, but perhaps even more burdensome in the export setting. The robust exports controls and sanctions regime deployed by the U.S. government over the past decade has added compliance costs for U.S.-based manufacturers, especially so given that the cost of noncompliance includes not just civil or administrative penalties but possible criminal indictments for certain illegal conduct.

In 2024, the associated compliance burden expanded in scope with the enactment of the 21st Century Peace through Strength Act, which President Biden signed into law in April 2024. Section 3111 of the Act extends from five years to 10 years the statute of limitations for civil and criminal violations of the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA). In July 2024, the Office of Foreign Assets Control (OFAC) published guidance stating that it "may now commence an enforcement action for civil violations of IEEPA- or TWEA-based sanctions prohibitions within 10 years of the latest date of the violation if such date was after April 24, 2019." Correspondingly, OFAC introduced an interim final rule on September 11, 2024, amending the Reporting, Procedures and Penalties Regulations to increase the recordkeeping requirements to 10 years to align with the statute of limitations for civil and criminal violations.

By expanding the statute of limitations, the U.S. government has significantly moved the compliance goalposts for manufacturers. Compliance programs will now need to contemplate conduct on a longer timeline with all of the associated recordkeeping requirements. But that longer timeline could have less obvious implications, as well. Having a "reasonable" risk-based compliance program often figures prominently in whether OFAC decides to mitigate the penalties it assesses when it uncovers a violation, but reasonableness is a fluid concept. What seemed reasonable in 2022 might not seem so to OFAC in 2032 with the benefit of 10 years of hindsight. Manufacturers will need to be alert to all the implications an expanded statute of limitations and recordkeeping requirements may have on their operations.

This change in law is consistent with the U.S. government's ongoing efforts to ramp up enforcement of its steadily growing exports controls and trade sanctions regime. For instance, in February 2024, OFAC and the Department of State jointly announced more than 500 sanctions designations targeting government officials, companies, and individuals in Russia and beyond. The sanctions illustrate how U.S. trade policy has evolved to address not just economic concerns but also to signal U.S. displeasure with the geopolitical aims of foreign governments. The sanctions primarily targeted Russian government officials responsible for the death of Aleksey Navalny—a Russian opposition politician who died in February 2024 while in prison—as well as entities in Russia's military-industrial base, entities providing revenue to the Russian government to support its military, and companies and individuals throughout Europe, Asia, and the Middle East considered to be aiding Russia in its efforts to evade sanctions.

As OFAC and the Department of State were expanding U.S. sanctions, the Department of Commerce's Bureau of Industry and Security (BIS) added 93 entities and over 900 parties from Russia, China, Turkey, the UAE, Kyrgyzstan, India, and South Korea to its Entity List. BIS also expanded from 45 to 50 the number of high priority items subject to Export Administration Regulations (EAR). These entities are subject to a license requirement for all items subject to the EAR and a license review policy of either presumption of denial or policy of denial for all items subject to the EAR.

Additionally, BIS **released guidance in August 2024** highlighting the various mechanisms it has employed—outside of its usual public screening lists—to notify companies and universities about parties that present

risks of diversion to Russia. These include letters and notices with information drawn from a variety of sources, including government data, news reports, open-source reports, and information learned from the exporter community at large. Importantly, BIS will consider as an aggravating factor in any enforcement action an organization's decision to proceed with a transaction (without obtaining an export license) when the company or university knew or had reason to know or believe that a red flag exists which could not be affirmatively addressed or explained.

Cortney Morgan

is a Washington-based partner in Husch Blackwell's Technology, Manufacturing & Transportation group and leads the firm's International Trade and Supply Chain practice, focusing her practice on the production, sourcing, and movement of goods, services and technology across international borders.

Dan Wilson

is a partner in Husch Blackwell's International Trade and Supply Chain practice based in Washington, advising clients on a variety of complex trade matters, including antidumping and countervailing duty proceedings and high-stakes enforcement matters before U.S. Customs and Border Protection.

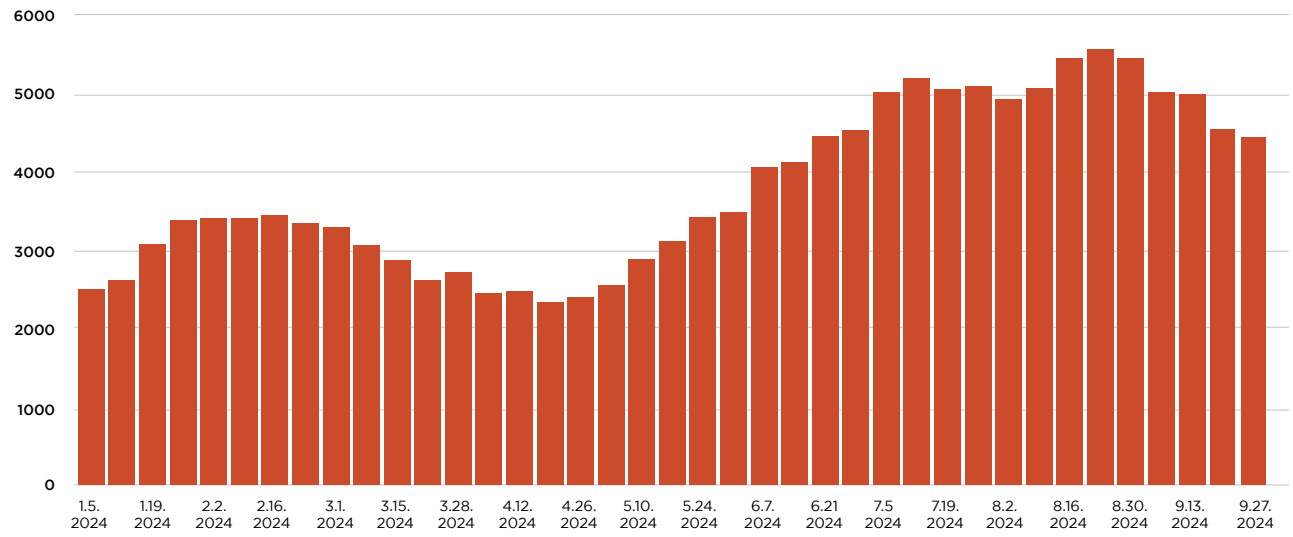
Transportation & Logistics

JULIE MAURER AND LOREN UNGAR

After a period of relative calm in 2023, this past year witnessed a variety of disruptions underscoring the fragility of global supply chains amid a larger reconfiguration of world trade.

Nearly one-third of industry leaders surveyed by the National Association of Manufacturers in June 2024 cited transportation costs as their primary business concern, reflecting ongoing geopolitical and logistical challenges that have led to steadily higher shipping rates throughout the year. Despite expectations that new capacity would eventually provide shippers with relief, the higher rates have been sticky. As 3Q 2024 drew to a close, the Freightos Baltic Index (FBI) hovered at or near $5,000. While a return to Covid-era rates is unlikely (the FBI peaked in September 2021 at just over $11,000), current levels are much higher than year-end 2023 rates and have contributed to elevated operating costs.

FREIGHTOS BALTIC INDEX (FBX): GLOBAL CONTAINER FREIGHT INDEX
Index in U.S. Dollars



Source: *Freightos.*

Detention & Demurrage

By the end of 2023, with supply chains returning to something close to normal, detention and demurrage (D&D) charges had fallen back to pre-pandemic levels after experiencing a tenfold run-up during Covid. Recent disruptions, however, could reverse this trend.

It was during the Covid-related spike in D&D charges that Congress passed the Ocean Shipping Reform Act of 2022 (OSRA), which sought to even the playing field between carriers and shippers by reforming the invoicing process to provide all parties with clarity, predictability, and timeliness in the assessment of D&D charges.

In February 2024, the Federal Maritime Commission (FMC) published a **final rule** in connection with D&D billing practices, and the rule took effect May 28, 2024. The rule **sets forth** the process for invoicing, including who can be invoiced, the minimum information required for compliant invoices, the timing of invoices, and when an invoice can be timely contested by the billed party. Notably, these regulations affect not only shippers and carriers but also Non-Vessel Operating Common Carriers (NVOCCs), steamship companies, customs brokers, warehousemen, and truckers—in short, the complete supply chain.

In April 2024, the World Shipping Council (WSC), a carrier trade association, filed a petition for review with the D.C. Court of Appeals challenging FMC's final rule as "arbitrary, capricious, an abuse of discretion, and otherwise contrary to law," as well as seeking an order vacating the final rule. This case and other potential administrative challenges to transportation regulators will be closely watched especially in light of the recent U.S. Supreme Court decision in *Loper Bright*.

Given the wide application of Chevron in administrative law over the past 40 years, it is anticipated that the full impact of Loper Bright in the transportation space will play out in the courts, the legislature, and administrative agencies for years to come. For instance, we could see future actions that attempt to curtail the U.S. Department of Transportation's (DOT) authority to define an "unfair and deceptive practice" or challenge the National Transportation Safety Board's investigative policies following accidents.

$13.8 billion

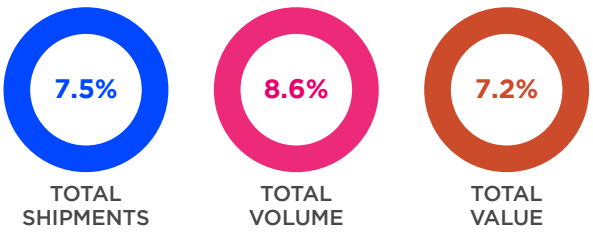
Detention and demurrage fees charged between April 2020 and September 2023 by the nine carriers participating in FMC's VOCC Audit Program.

Private Fleets Versus Outsourcing

Over the past decade, episodes of severe scarcity in trucking capacity have plagued the freight markets, leading many manufacturers to implement—or at least, to consider implementing—private fleets. The use of private fleets has waxed and waned over time, along with the underlying economics of building and maintaining what is—for most manufacturers—a truly non-core capability. As manufacturers revisit this perennial question, there are some factors and trends worth considering.

At the top of the list is cost, which is often decisive. The structural overhead associated with trucking has increased, with driver compensation, insurance, fuel, and vehicle purchase and maintenance all experiencing significant inflation over the past decade. This escalation in cost would argue against private fleets, but trends have moved in the opposite direction since the onset of Covid, mostly because the negative effects of not being able to transport product during periods of extreme supply-chain dislocations can be enterprise-threatening; thus, private fleets operate as a kind of hedge against certain geopolitical, logistical, and trade-related risks.

YEAR-OVER-YEAR INCREASES IN PRIVATE FLEET UTILIZATION



Source: *National Private Truck Council, 2024 Benchmarking Survey Report.*

Just as the total cost of ownership for private fleets have increased, so, too, have the associated legal and regulatory challenges. In addition to the myriad standard trucking industry compliance areas—such as hours of operation, vehicle inspections and maintenance, cargo handling, driver qualifications, and incident tracking—there are novel regulatory initiatives that will add cost and consume resources for those engaged in trucking. These efforts are typically found in areas relating to sustainability and safety and include stricter federal and state emissions standards, enhanced drug and alcohol testing policies, and the increased (and mandated) use of Electronic Logging Devices (ELDs).

Private fleet operators also have exposure to fast-evolving risks that are difficult to measure and manage. As the mandated use of ELDs accelerates, the trucking industry increasingly relies on complex tech systems and network interconnectedness with its rolling assets. Fleet owners need to take adequate cybersecurity countermeasures to anticipate social engineering and phishing attacks, application programming security, and vulnerabilities in trucking technology, including data privacy protections.

Additionally, the operation of private fleets adds a layer of complication to an already complex web of labor and employment law. Operators must be knowledgeable and aware of the state and federal rules affecting the independent contractor classification of certain drivers and other trucking agents. Recent state laws, such as those in California, Massachusetts and New Jersey, and the 2024 U.S. Department of Labor final rule regarding whether a worker is an employee or an independent contractor under the Federal Fair Labor Standards Act can make the economic reality of hiring a difficult one.

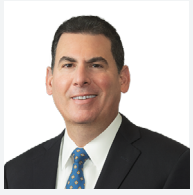
There is no single answer to the private fleet conundrum that will work for all manufacturers. For some, the goods and products moved will require highly customized containers, such as climate-controlled units, while other manufacturers might value control over delivery and customer service above all else. The risks and rewards of private fleets will necessarily be different from operation to operation, but the dilemma is not an either/or proposition. Hybrid solutions that mix outsourcing with private fleets allow manufacturers great flexibility in managing its transportation needs.

UPDATE ON ILA STRIKE

On October 3, 2024, the International Longshoremen's Association (ILA) and the United States Maritime Alliance (USMX) reached an agreement that extends the ILA labor agreement that ended September 30, 2024, and that allows dockworkers to suspend their strike that affected East and Gulf Coast port operations. The extension will be in force until January 15, 2025. In the interim, negotiations will continue toward a new agreement.

Julie Maurer

is a Phoenix-based partner in Husch Blackwell's Transportation industry group. She has over two decades of experience handling legal matters for transportation and transportation-adjacent companies, including contract drafting and analysis, day-to-day legal consultations, regulatory advice, and complex litigation, often involving lost, damaged, or delayed cargo. She also serves as national coordinating counsel for many of the top transportation and logistics entities around the globe.



Loren Ungar

is a member of the firm's Transportation industry group and draws on 20 years of experience as a litigator to represent transportation clients in complex commercial disputes, including trade secret cases, class action defense, breach of contract disputes, fraud allegations, shareholder and partner disputes, and investor actions.

Corporate Transactions

ASHLEY EDWARDS

Enthusiasm for dealmaking is growing ahead of anticipated cuts to interest rates, which could vastly improve deal flow heading into 2025.

Much like the narrative surrounding the larger economy, dealmaking in the first half of 2024 was a mixed bag of good and bad news. Overall sentiment is improving as first-half deal values in the U.S. and globally edged up, but concerns among dealmakers persist as the second quarter failed to keep pace. Both strategic and financial deal participants have consistently cited **valuation as a major hurdle**, and to be sure, financial markets have experienced significant volatility, even as they push against all-time highs. In August 2024, the CBOE Volatility Index, or VIX, experienced an unprecedented seesaw, posting its biggest intraday jump in history, followed by its largest six-day decline, highlighting the fragility of markets as they test valuation limits.

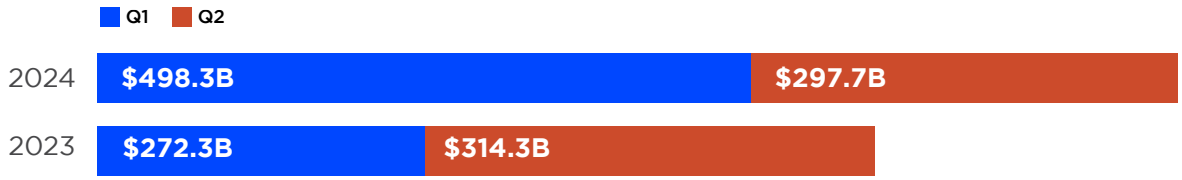
The valuation gap between buyers and sellers has also fed on factors not related to the market as a whole. Post-Covid consumer demand and patterns of consumption have been wildly unpredictable, adding a level of complexity to sellers rationalizing large swings in revenue and projecting future corporate earnings. Inflation and rising costs of materials and labor have had a dramatic effect on some companies' historic financials. Finally, technological innovations, such as generative artificial intelligence, are leading to large expenditures for some companies, while at the same time making it difficult to pin down how exactly these rapidly evolving innovations will reconfigure operations. These factors have played a role in creating frothy markets and suppressing manufacturing industry deal values and volumes.

Despite these challenges, deals are still being closed in certain corners of the wider market. Areas of strong deal activity include all-domestic transactions, which accounted for 80 percent of all deals closing from January to April 2024—10 percentage points higher than the historical average. According to PwC's **Industrial Manufacturing: US Deals 2024 Midyear Outlook**, this spike in domestic activity reflects measures taken by U.S. companies to address "supply chain management risk driven by geopolitical uncertainty."

Using Earnouts to Close Valuation Gaps

The PwC report also noted the continuing strength of middle-market and strategic bolt-on transactions in the U.S., segments that also prominently feature private companies where owners are looking to exit. Private company valuations are

U.S. M&A DEAL VALUES, H1 2023 VS. H1 2024



Source: *LESG and Axios.*

notoriously difficult and can be a major sticking point in the deal process; however, there are some approaches to managing valuation risk in these instances. The use of earnouts—which tie a portion of the purchase price to some future financial metric—is often seen in private company deal structures and can help close the valuation gap in negotiating deals.

It should be noted that, while the inclusion of earnout provisions can plug the valuation gap during the negotiation phase, it can lead to disputes post-closing when it comes to operating the business and determining whether the earnout measure was achieved. It is not always true that the interests of buyers and sellers remain in alignment after the deal is closed; therefore, purchase agreements should clearly outline the rights and restrictions of the parties that will govern during the earnout period and explicitly account for situations where the objectives of the buyer and seller may fall out of alignment.

Earnouts are complex structures that require sharp attention to detail and an ability to think through complicated macroeconomic and industry-specific data, as well as the structure's tax implications. Both buyer and seller should consider the tax consequences associated with best-case and worst-case scenarios and how those affect the economics of the deal.

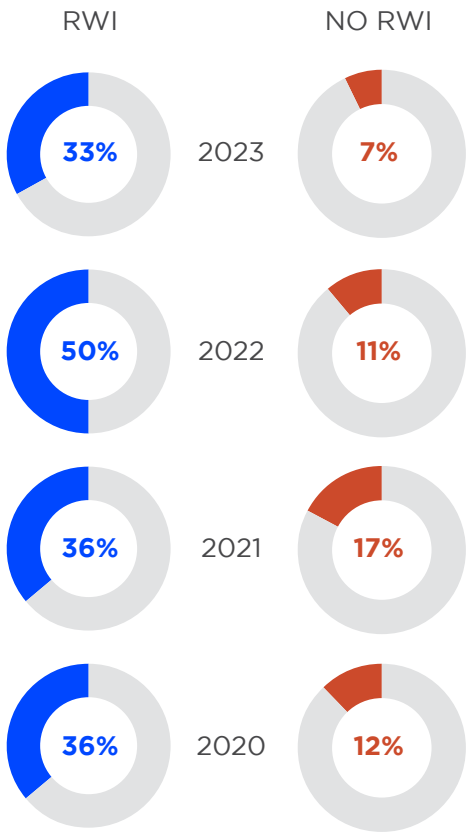
The Role of Representations and Warranties Insurance

Another method of hedging transaction risk involves the use of Representations and Warranties Insurance (RWI). For buyers, the obvious utility of RWI is to guard against breaches of representation and warranties without having to pursue the seller or require the seller to tie up a large part of the purchase price in an escrow for an extended period of time. RWI policies typically range between 10 to 20 percent of the purchase price, thereby offsetting transaction risk without the need for a large escrow. Furthermore, policies can be customized to cover a desired timeframe with premiums that flex accordingly. The presence of RWI often signals to the seller a buyer's seriousness and attention to detail, making a buyer's proposal more competitive. Another benefit is, when previous owners remain involved with the business post-closing, RWI can prevent a buyer from having to pursue an awkward indemnity claim against the previous owner who is now a part of buyer's organization.

The presence of RWI can limit or eliminate the need to hold funds in escrow for indemnity claims. Sellers prefer clean exits and have therefore displayed a greater preference for bids including RWI. RWI also reduces some pressure on the negotiation of reps and warranties and certain indemnity provisions in a purchase agreement, thereby relieving both buyer and seller of a major pain point in the negotiation process.

All hedges come with certain tradeoffs, and RWI is no different. RWI claims can take as long—and sometimes longer—to resolve as traditional indemnity claims, and they can entail more complexity. According to SRS Acquiom, an M&A consultancy, RWI can also influence deal terms: deals with RWI are more likely than deals without RWI to be structured as "no

PERCENTAGE OF M&A WITH NON-SURVIVAL TERMS



Source: *Atlantic Global Risk LLC.*

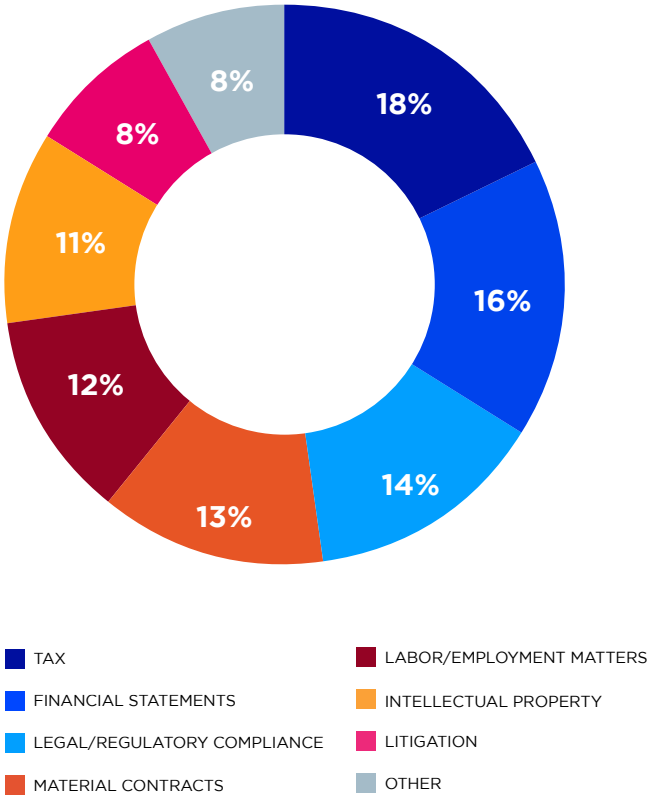
survival," that is, deals where the seller's representations and warranties do not survive beyond the closing.

While underwriters work with deal participants to craft a policy appropriate to the desired coverage levels and stated risk appetite, there are certain risks that will fall outside the scope of RWI. Among those areas, known issues (known as "deal-specific exclusions") and "actual knowledge" of the buyer's deal team are at the top of the list, meaning RWI policies typically will not cover issues known to the buy side through its diligence or some other means. Additionally, purchase price adjustments, transfer pricing issues, asbestos-related claims, and pension withdrawal issues almost always fall outside the scope of coverage.

Once upon a time, RWI was only seen in larger transactions, but more and more, it is found in smaller deals well under $100 million. Given that much of the deal activity in the manufacturing industry has featured smaller, bolt-on acquisitions or middle-market transactions, carriers are working to take advantage of the increased demand by developing insurance products specifically tailored to smaller deal sizes.

These streamlined RWI policies could offer valuable protection, particularly for companies—both strategic acquirers and those with a private equity sponsor— that aggressively use M&A to grow. Even the limited scope of the most standard items included in RWI, like tax-related claims and regulatory compliance issues, can provide deal teams some comfort as they perform diligence in connection with evolving areas of risk, such as supply chain-related areas, labor and employment law, or the way an enterprise operationalizes artificial intelligence.

MOST FREQUENT RWI CLAIMS



Source: *Atlantic Global Risk LLC.*

Ashley Edwards

is a St. Louis-based partner in Husch Blackwell's Technology, Manufacturing & Transportation group. She has closed over $65 billion in corporate M&A transactions and represents private financial and strategic buyers and sellers in a variety of industries, primarily focusing on consumer goods and manufacturing.