HUSCH BLACKWELL

Legal Insights for Manufacturing

A look ahead at the issues that will shape 2024 for the manufacturing industry

NOVEMBER 2023

Introduction

With each passing day it becomes more apparent the world that entered the Covid-19 pandemic is not the world that emerged from it.

Two characteristics that have defined the 21st century's global economy—historically low interest rates and the Chinese economic 'miracle'—have reversed course over the past year. Interest rates experienced the fastest hike in modern history, rising nearly 500 basis points in 14 months. Meanwhile, China's economy has noticeably slowed, weighed down by its prolonged Covid countermeasures, real estate woes, a decline in global demand, and a reshuffling of global trade due in part to an unravelling of the geopolitical order.

Amid the rising cost of money and an ongoing reconfiguration of global supply chains, U.S. manufacturing has experienced pockets of strength but is struggling to grow broadly. For most of the past of 12 months the sector has declined, according to the J.P.Morgan Global Manufacturing PMI. Moreover, forward-looking indicators, such as measures of future output, new orders, and existing inventory, do not suggest short-term improvement.

These macroeconomic challenges are amplified in the U.S. by rapid growth in the scope and complexity of government regulation. Regulatory efforts have advanced along multiple lines, introducing complications for corporate transactions, labor and employment matters, market behavior, and cybersecurity, among other areas. Moreover, regulatory overlap—from agency to agency or between the local, state, and federal levels of government—has created profound confusion and spawned ever-greater levels of complexity for compliance teams to ponder.

Our second-annual *Legal Insights for Manufacturing* report seeks to explore selected trends of great importance and provides perspective that informs how manufacturing leaders can respond to different kinds of change—both the large generational forces that are redrawing the map, as well as the day-to-day changes that affect businesses in a material, albeit more modest, fashion. We hope the information presented here can help inspire the creativity U.S. manufacturers will need to meet the challenges that lie ahead.

Jeffrey Sigmund

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

Setting the Agenda

Throughout the first half of 2023, manufacturers' worries regarding supply chain dislocations and burgeoning transportation costs ebbed, replaced by concerns over potential weakness in demand and heightened regulatory activity.

Many of the challenges that had aroused intense concern throughout 2022 have greatly decreased in urgency. Post-Covid supply chain dislocations were chief among them, along with general price inflation and transportation costs. Each of these have moderated. Even before 2022 had ended, the volatile energy and food components of the inflation gauge had turned markedly south, bringing headline inflation down as well. Likewise, as 2022 dawned, global container freight rates were near all-time highs—about fivefold higher than pre-pandemic levels. By the end of the year, they had returned to something close to normal. No surprise, then, that surveys of manufacturing leaders show a dramatic decline in the level of concern these challenges merited at the mid-year mark of 2023.

PRIMARY CURRENT BUSINESS CHALLENGES

	2Q23	4Q22	% Change
ATTRACTING AND RETAINING A QUALITY WORKFORCE	74.4	75.7	-1.3
WEAKER DOMESTIC ECONOMY AND SALES FOR OUR PRODUCTS	55.7	47.6	8.1
RISING HEALTH CARE/INSURANCE COSTS	53.1	47.9	5.2
UNFAVORABLE BUSINESS CLIMATE (E.G., TAXES, REGULATIONS)	52.1	44.1	8.0
INCREASED RAW MATERIAL COSTS	50.8	60.7	-9.9
SUPPLY CHAIN CHALLENGES	44.9	65.7	-20.8
TRANSPORTATION AND LOGISTICS COSTS	29.5	50.0	-20.5
WEAKER GLOBAL GROWTH AND SLOWER EXPORT SALES	20.7	24.0	-3.3
TRADE UNCERTAINTIES	18.7	21.9	-3.2
CHALLENGES WITH ACCESS TO CAPITAL/FINANCING	7.9	8.6	-0.7

Source: National Association of Manufacturers, NAM Manufacturers' Outlook Survey (January 2023 and June 7, 2023)

Taking their place, however, was a more generalized concern regarding demand and the costs associated with regulatory compliance. On the demand front, 1H2023 data suggest resiliency in consumer spending that has buoyed growth and helped ward off recession worries, at least through midyear; however, the support provided by stimulus-related excess savings and the pause in student-loan debt service is nearing its end. Lower levels of consumer support—plus fears of an inflation rebound—could make for a challenging 2024. As ever, regulation is also a major concern, especially so given its rapid growth in scope and complexity across virtually all areas of operation. We do not anticipate a lessening of this burden in the short run for U.S. manufacturers; if anything, the complexity and costs are likely to rise from current levels and will challenge manufacturers, especially smaller and middle-market companies.

FEDERAL REGULATORY BURDEN FOR U.S. MANUFACTURERS

Mfg. Process Step	Federal Regulations*	Number of Restrictions
HEALTH & SAFETY	85	102,734
TAX	26	51,760
PRODUCTION	239	44,628
QUALITY CONTROL	83	23,951
DISTRIBUTION & SHIPPING	64	21,057
HUMAN RESOURCES	54	17,042
R&D/NEW PRODUCTS	22	12,833
GOVERNANCE	8	8,884
LABELING & PACKAGING	47	7,477
SOURCING	43	4,168
POST-SALE FOLLOW-UP	9	1,644
MARKETING & SALES	35	1,518

*Denotes the number of parts of code of federal regulations.

Source: National Association of Manufacturers, "Holding Us Back: Regulation of the U.S. Manufacturing Sector" (2017)

Table of Contents

Labor & Employment

Amid declining productivity, rising labor costs, aggressive tactics from organized labor, and a scarcity of skilled labor, the employment regulatory landscape continues to present challenges for manufacturers.

Over the past year the competition for talent has remained intense. While manufacturers would prefer to invest in upgrading employee experiences to achieve employee loyalty, the increasing pace of change in the law governing the employer-employee relationship demands that more attention is given to policy review and training on practices to avoid legal pitfalls. In the meantime, unions are exploiting these changes to increase unionization efforts and seek greater leverage at the bargaining table. In last year's report, we highlighted the nationwide spike in unionization efforts and the potential for strikes, given the level of general price inflation and the Biden administration's affinity for organized labor. Through the first eight months of 2023, the manufacturing industry saw 28 strikes involving over 11,500 striking workers, according to the **Cornell University Worker Institute Labor Action Tracker**. This represents a 33 percent increase in the number of strikes over the same time period during the previous year.

NLRB Expands Section 7 Coverage

Despite the popular narrative concerning a renaissance of organized labor, the 2022 union membership rate (10.1 percent) is the lowest on record. Still, public policy and regulation have not moved in management's favor. For instance, in August 2023, the National Labor Relations Board (NLRB) introduced new obligations for employers when a union demands voluntary recognition. Traditionally in this setting employers have rejected union claims of majority status and have refused to voluntarily recognize, forcing the union to use the election process under the National Labor Relations Act (NLRA). After all, employers will never know the veracity of the authorization cards used in seeking voluntary recognition, how the union obtained the cards, or what the union might have told employees in

Labor Organizations Participating in 2023 Work Stoppages*

- Bakery, Confectionery, Tobacco Workers and Grain Millers International Union (BCTGM)
- IUE-CWA
- International Association of Machinists and Aerospace Workers (IAM)
- International Chemical Workers Union
- International Chemical Workers Union Council (ICWUC)
- Laborers' International Union of North America (LiUNA)
- Teamsters (IBT)
- United Auto Workers (UAW)
- United Electrical, Radio and Machine Workers of America (UE)
- United Food and Commercial Workers Union (UFCW)
- United Steelworkers (USW)
- Venceremos

*Through August 31, 2023. Manufacturing industry work stoppages only.

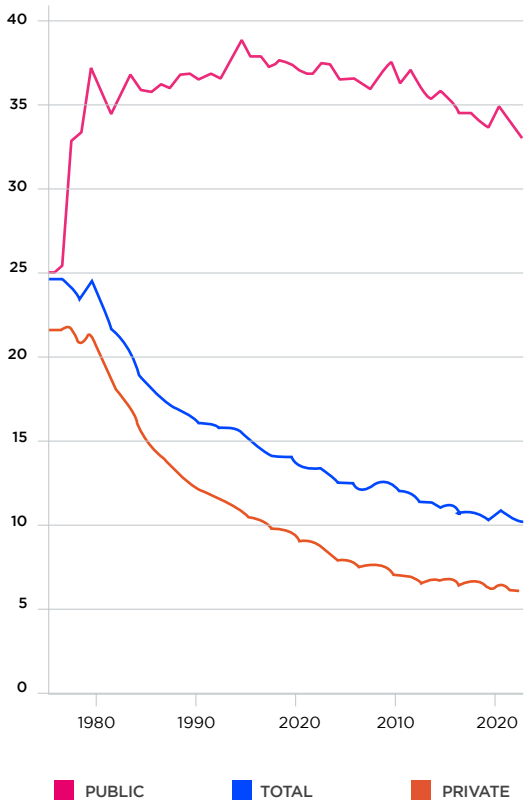
exchange for a signature. In the face of a union's request for voluntary recognition, an employer will often tell the union to file a petition for an election so employees may cast their ballot in a NLRB supervised election, free of coercion and undue influence. Even if employees have signed cards, employees are free to change their minds and vote their consciences in a NLRB secret ballot election.

This approach of declining or ignoring requests for voluntary recognition will no longer be appropriate, given the NLRB's decision in *Cemex Construction Materials Pacific, LLC* (August 2023), which introduced a new framework for how employers respond to a union's demand for voluntary recognition and the Board's authority to issue a bargaining order based on that response and based on an employer's behavior during the election's critical period. Under the new framework, when a union requests recognition on the basis that a majority of employees in an appropriate bargaining unit have designated the union as their representative for the purpose of collective bargaining, an employer must either (1) recognize and bargain with the union or (2) promptly file representation management petition seeking an election. The employer cannot simply ignore the demand and cannot follow the traditional advice of telling the union to file its own election petition.

Additionally, the NLRB has raised the stakes for employers who choose the election route. If an employer seeks an election and thereafter commits any unfair labor practice that would require setting aside the election, the petition will be dismissed. More importantly, rather than re-running the election, the Board will issue an order requiring the employer to recognize and bargain with the union.

Cemex forces employers to take action and will likely chill employer campaign activities designed to educate employees about the election process, the choice as to whether unionization is right for them, and the consequences of a vote in favor of union representation. Despite the likelihood that *Cemex* will be tested and decided in the courts, employers need to develop new approaches to respond to a union's demand for voluntary recognition.

PERCENTAGE OF WORKFORCE WITH UNION MEMBERSHIP

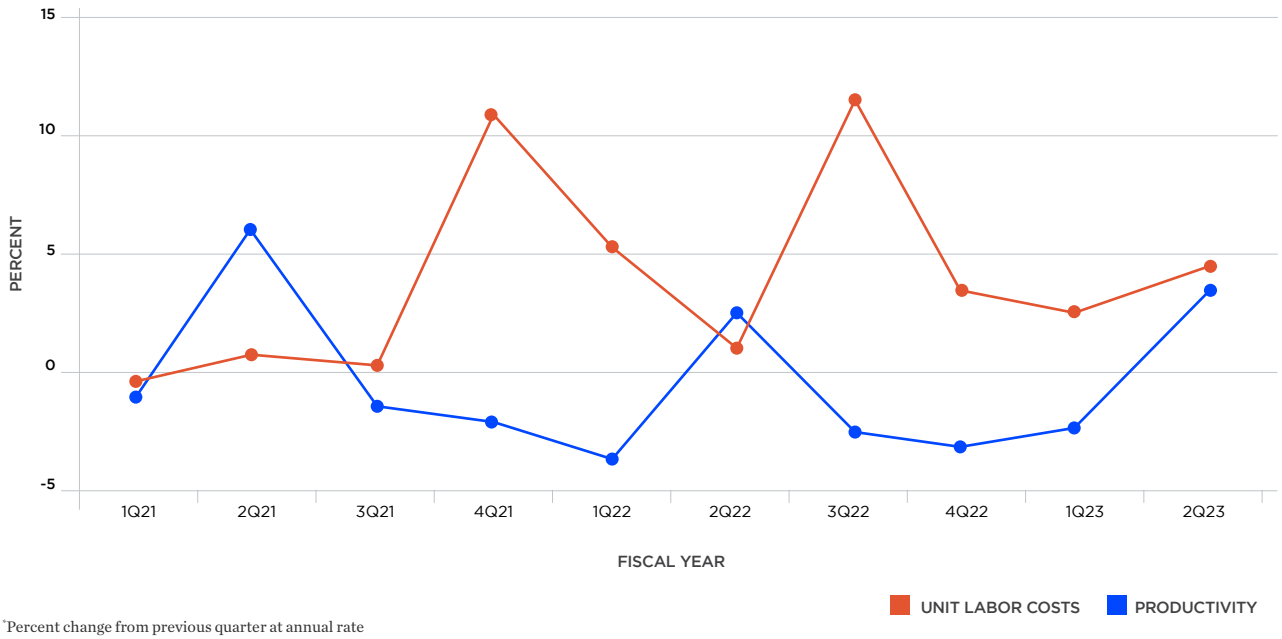


Source: U.S. Bureau of Labor Statistics

Cemex is not an isolated development, but rather another expression of the Biden administration's labor-friendly approach to policymaking. The Board's 2023 decisions and guidance have consistently forwarded organized labor interests, chiefly by widening the ambit of "protected concerted activity" under Section 7 of the NLRA. For example, in August 2023, the Board handed down a decision in *Stericycle, Inc.*, introducing a new standard for workplace rules that dramatically restrict what employers can mandate. In *Stericycle* the Board reverted to a central framework of finding that a workplace rule violates the NLRA if it has a "reasonable tendency to chill employees from exercising their Section 7 rights." Enforcement of a rule to specifically stifle protected conduct is not required; merely maintaining an overbroad work rule violates the Act, according to *Stericycle*.

POST-COVID PRODUCTIVITY AND UNIT LABOR COSTS FOR U.S. MANUFACTURING*

Labor costs have exceeded productivity gains in eight of the last 10 quarters.



*Percent change from previous quarter at annual rate

Source: U.S. Bureau of Labor Statistics

The *Stericycle* decision works hand in glove with prior Board decisions to circumscribe management's ability to, well, manage. While *Stericycle* addresses workplace rules, a May 2023 decision in *Lion Elastomers and United Steelworkers* makes it more difficult for employers to discipline employees for outbursts and similar misconduct while employees are engaged in "protected concerted activity." As a practical matter, *Lion Elastomer*s removes most boundaries around what employees can say or do, so long as the Board construes the actions as falling within the scope of protected activity.

For manufacturers who routinely have to weigh and balance multiple shop-level or factory floor concerns, such as employee safety, the continuing evolution of Section 7 rights—both by Board decisions and by NLRB General Counsel memoranda—does not make the task of managing employees easier.

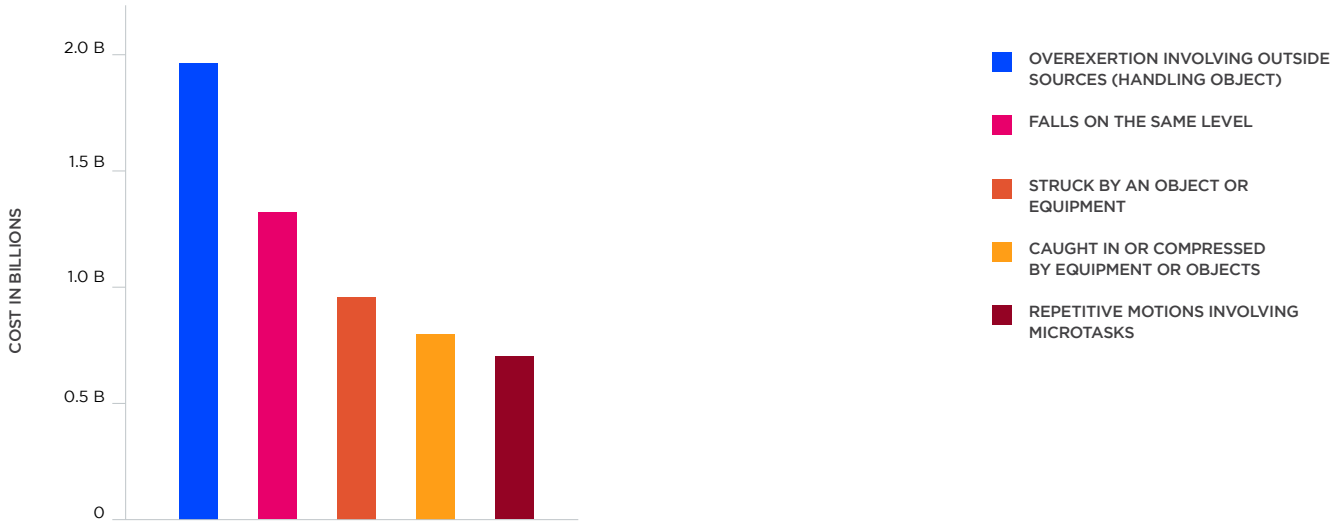
Workplace Safety

Traditionally, workplace health and safety regulation has represented the largest share of federal law restrictions placed upon manufacturers, and as 2023 dawned, the Occupational Safety and Health Administration (OSHA) was busy adding to the mountain of existing regulation. The agency had nearly two dozen regulations in various stages of rulemaking on its annual agenda and is actively moving along rules that many manufacturers will find burdensome.

For instance, earlier this year, OSHA greenlighted a policy whereby regional offices can issue multiple citations—so-called Instance-By-Instance, or IBI, citations—for each separate violation stemming from a single investigation. These citations could carry separate associated penalties as well. These penalties, of course, would be in addition to the compliance costs and insurance claims associated with workplace injuries. The manufacturing industry loses approximately $8.5 billion per year to serious, non-fatal workplace injuries, according to Liberty Mutual Insurance.

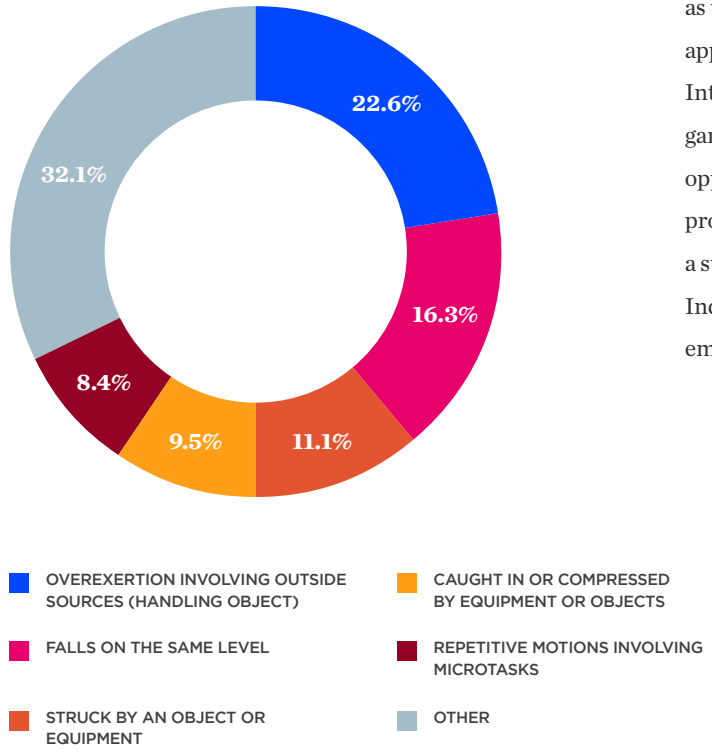
The agency also advanced new rules in August permitting non-employee representatives during OSHA inspections, provided they are "reasonably necessary to conduct an effective and thorough inspection." The rulemaking also revived OSHA's efforts to allow non-unionized workers the ability to designate outside third parties affiliated with a union

TOP 5 COSTLIEST MANUFACTURING WORKPLACE INJURIES*



TOP 5 COSTLIEST MANUFACTURING WORKPLACE INJURIES*

As percentage of total workplace injuries



as their representatives during OSHA inspections. This approach—outlined in the Fairfax Memo, a 2013 Letter of Interpretation—has drawn the ire of employers who see the gambit as an attempt to use OSHA inspections as a backdoor opportunity to unionize outside of the traditional bargaining process. OSHA rescinded the Fairfax Memo in 2017 following a successful legal challenge by the National Federation of Independent Business but appears to be making another run embedding organized labor in non-union shops.

*Non-fatal workers compensation claims with more than five days away from

Source: Liberty Insurance Company. https://business.libertymutual.com/wp-content/uploads/2022/06/WSI-1005_2022.pdf

Regulatory & Compliance

Complying with the ever-greater demands of government regulation continues to weigh on manufacturing leaders, particularly in middle-market companies that cannot easily scale compliance costs.

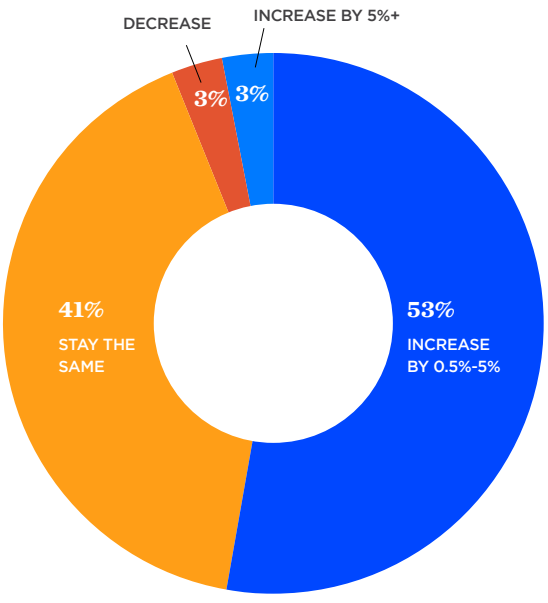
Across the whole of government, regulators have ramped up oversight of private businesses, and manufacturing is no exception. Industry leaders continue to cite government regulation as a primary challenge, and it is well established that the burden of compliance falls most heavily on middle-market and smaller enterprises, which generally lack the ability to scale compliance efforts to contain costs.

These burdens are not likely to ease any time soon. According to the 2023 KPMG Chief Ethics & Compliance Officer Survey, 73 percent of respondents perceive "increasing regulatory expectations and scrutiny." Correspondingly, only three percent of those surveyed foresee decreasing headcount tasked with compliance functions.

In addition to increasing FTEs related to compliance, chief compliance officers (CCOs) also anticipate budget increases to build out technology and data analytics, cybersecurity systems, and artificial intelligence capabilities. This dynamic is not exclusive to manufacturing, as surveys of leaders across various industries—especially financial services—demonstrate a similar desire to enhance the compliance function.

As one might imagine, the demand for compliance professionals runs the danger of outstripping supply. Nearly a quarter of CCOs note that attracting capable talent is a challenge, one that is likely to grow amid the surge in regulatory activity. Notably, more and more companies are looking to outsource some or all of their compliance function. The approach is particularly attractive for middle-market companies where the need for specific subject-matter expertise and/or data analysis is high and where the cost of building an in-house team or technology stack lacks a firm economic basis.

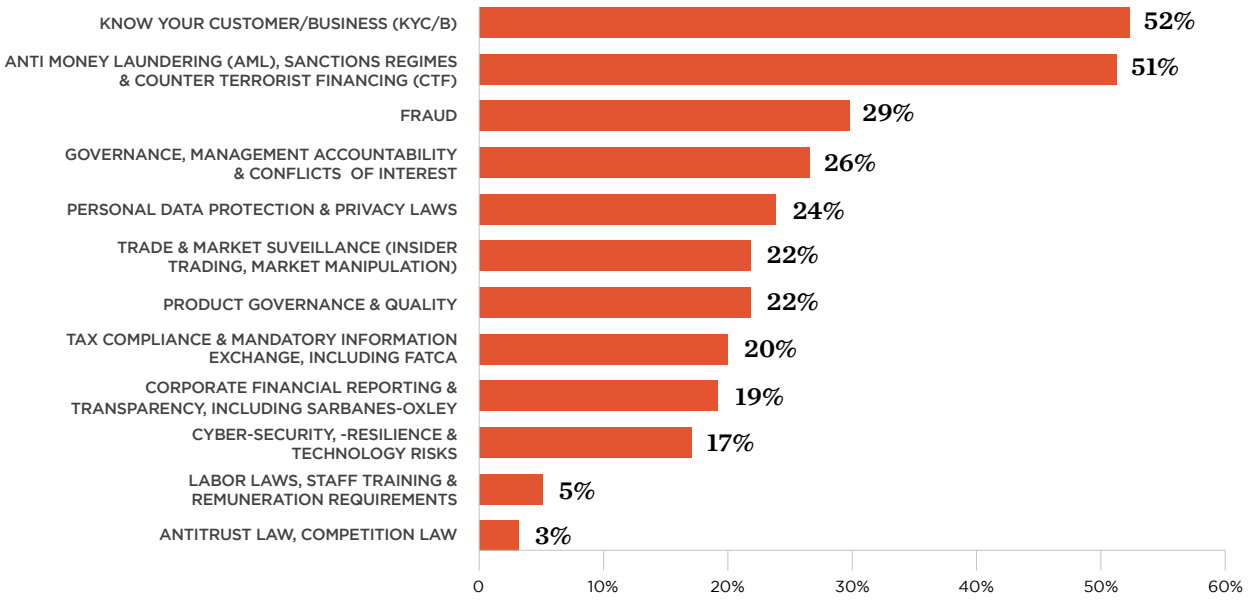
ANTICIPATED COMPLIANCE FTE FOR 2024



Source: 2023 KPMG Chief Ethics & Compliance Officer Survey

MOST FREQUENTLY OUTSOURCED REGULATORY COMPLIANCE AREAS

Percentage of RegTech firms offering services per regulatory focus



Source: Cambridge Centre for Alternative Finance (CCAF), The Global RegTech Industry Benchmark Report.

Regulators have placed a heavy focus on building and maintaining strong compliance programs. The Biden administration's Department of Justice (DOJ) has been unequivocal on this point, providing official and unofficial guidance that reinforces the concept. For instance, in March 2023, the DOJ's Criminal Division revised its **Evaluation of Corporate Compliance Programs (ECCP)** guidance for the first time since 2020, placing new attention on two emerging areas: (a) the role of compliance in monitoring a company's use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications, and (b) the intersection of compliance with executive compensation.

That same month, Deputy Attorney General Lisa Monaco spoke to the American Bar Association National Institute on White Collar Crime and underscored the importance of compliance programs, particularly on the issue of compensation. She remarked that "[w]e want companies to step up and own up when they discover misconduct and to use compensation systems to align their executives' financial interests with the company's interest in good corporate citizenship."

While the ECCP guidance above pertains only to the Criminal Division, the deputy AG's numerous remarks make clear that all DOJ divisions are encouraged to embrace the focus on compliance programs; therefore, companies will need to assess the degree to which policies and related training will need to change in order to address risks. Clearly, the onus is being placed on private businesses—via their compliance programs—to self-monitor, and where such efforts are found lacking within the context of an investigation, regulators will be less apt to extend credit to companies or individuals.

INCENTIVIZING COMPLIANCE THROUGH COMPENSATION

The newly updated ECCP guidelines task prosecutors with looking at the following factors to determine if compensation is aligned with a compliance-friendly culture.

HUMAN RESOURCES PROCESSES

Concerns disciplinary procedures and decision making, transparency of internal and external communications, and consistency of application.

DISCIPLINARY MEASURES

Concerns the range of disciplinary actions available to management, including clawback policies, and the communication of these policies to company stakeholders.

CONSISTENT APPLICATION

Concerns the track record of the company in meting out compensation-based actions, as well as metrics applied by the company to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the organization.

> “Compensation structures that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance. At the same time, providing positive incentives, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership, can drive compliance.
>
> Department of Justice

FINANCIAL INCENTIVE SYSTEM

Concerns the intersection of financial rewards, company performance and compliance, including whether commercial targets are achievable if the business operates within a compliant and ethical manner and whether the compliance function has a role in designing and awarding financial incentives.

EFFECTIVENESS

Concerns the steps companies have taken to apply “consequence management” to compliance violations and the results of those actions.

Updates to FCPA Corporate Enforcement Policy

In January 2023, the Department of Justice announced updates to the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy. Since its inception in 2017, the FCPA Corporate Enforcement Policy has rewarded companies that self-regulate and self-report possible violations. Recent updates concerning DOJ's cooperation policy/guidance—which are meant to apply broadly to all investigations and/or prosecutions—further incentivize disclosure of FCPA misconduct and full and willing cooperation with an investigation. With a voluntary disclosure, full cooperation, timely and appropriate remediation, and full disgorgement, entities may be able to receive a declination of prosecution and greatly reduced sentencing, even when there are aggravating circumstances.

Beginning in 2019, DOJ offered presumptive prosecution declinations and reduced sentencing to companies to disclose FCPA violations and then cooperate with an investigation. Originally, "aggravating circumstances" automatically disqualified one from the declination. With the most recent update, a corporation may receive a declination, even if there are aggravating circumstances following specific corporate actions.

Similar to the original policy, corporations having committed misconduct with aggravating circumstances may receive a declination if they make a full, voluntary disclosure, had an effective compliance policy in effect at the time of the misconduct, and take "extraordinary" acts to cooperate with the Department.

In addition to allowing declinations even in light of aggravating circumstances, DOJ has increased the incentives for participating with the Corporate Enforcement Policy. Initially, participating offenders would get a 50% reduction from the low end of the sentencing guidelines fine range. Now, a fully cooperating entity can receive a reduction starting at 50%, going up to 75%, for complying with the Policy.

First, corporations having violated the FCPA must make a full, voluntary disclosure to the Department. Their disclosure should be "reasonably prompt" and reveal all "relevant, non-privileged facts." There can be no pre-existing obligation to disclose, and the disclosure must be "prior to an imminent threat of disclosure or government investigation."

Second, corporations must fully cooperate with the Department's investigation. The Department emphasizes cooperation must be proactive, as opposed to reactive. Corporations should make timely disclosures of facts and preserve and collect relevant documentation. Finally, when the Department investigates, the corporation should take steps for "de-conflictions of witness interviews and other investigative steps that a company intends to take" so they do not interfere with the Department's investigation.

Third, a timely and appropriate remediation is required. Corporations must conduct a "thorough analysis of causes of underlying misconduct." When the cause of misconduct is discovered, corporations must take measures to remediate and address the causes. Compliance programs should be implemented, if there is none. Employees should be disciplined as appropriate, and corporations should take "any additional steps that demonstrate recognition of the seriousness of the company's misconduct."

Finally, companies are required to pay disgorgement, forfeiture, and/or restitution to participate as a cooperator.

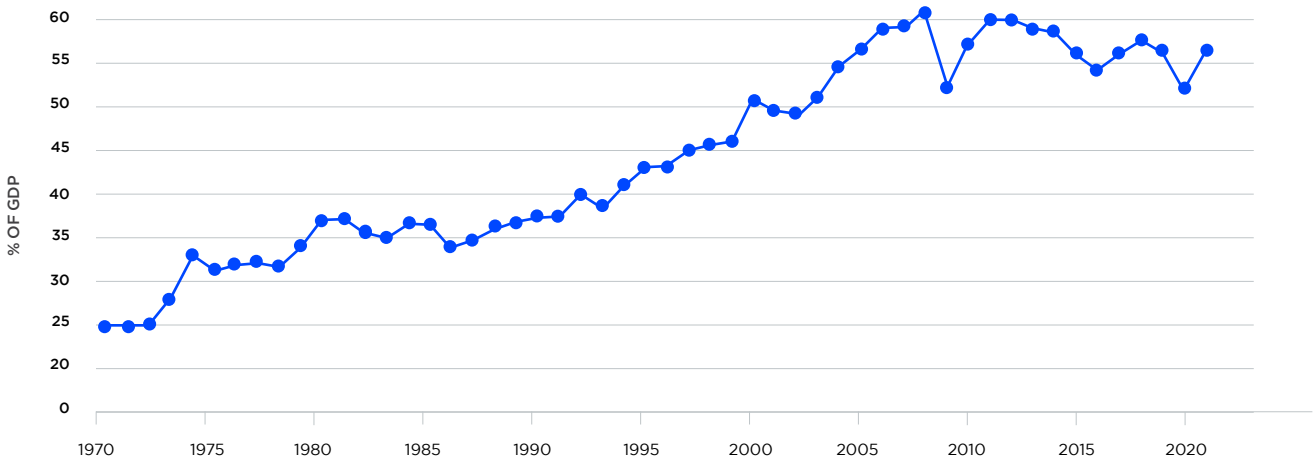
> "In assessing the quality of a cooperator's assistance, we value: when an individual begins to cooperate immediately, and consistently tells the truth; individuals who allow us to obtain evidence we otherwise couldn't get, like quickly obtaining and imaging their electronic devices, or having recorded conversations; cooperation that produces results, like testifying at a trial or providing information that leads to additional convictions.
>
> Kenneth Polite, Assistant Attorney General, in remarks at Georgetown Law Center, January 2023

International Trade & Supply Chain

Supply chain concerns and transportation costs have moderated since the summer of 2022; however, continuing geopolitical tension has led to greater regulatory scrutiny of international trade.

What a difference a year makes. Throughout most of 2022, inflation and supply chain dislocations ranked among the top challenges faced by the manufacturing industry, and while issues persist in some corners of the industry, the situation has been greatly ameliorated by falling prices and a shippers' market for transport. Still, uncertainties abound in the trade arena. Trade as a percentage of world GDP declined in eight of the 13 years prior to 2021, demonstrating a potential trend line toward deglobalization that predates and transcends both the Covid pandemic and the recent eruption of geopolitical tensions.

INTERNATIONAL TRADE AS A PERCENTAGE OF WORLD GDP, 1970-2021



Source: The World Bank

Voluntary Self-Disclosure of Trade Violations

Since peaking in 2008 as a share of world GDP, international trade has been increasingly used as a tool to express political disagreement with foreign regimes through the use of sanctions. As governments and multilateral institutions turn more frequently to sanctions of various kinds, it is private businesses that bear the burden of complying with the growing list of restrictions.

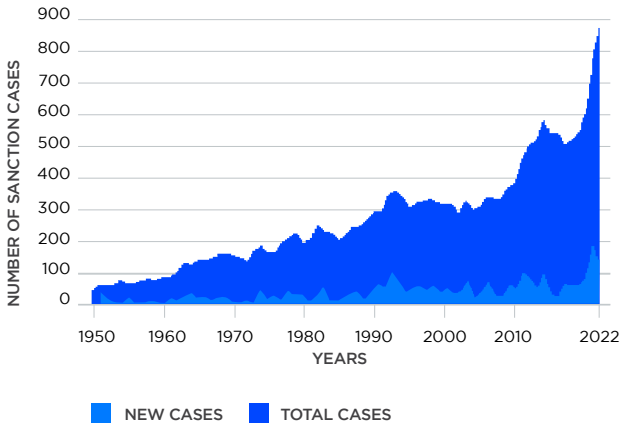
No government has the resources to police the entirety of international commerce; therefore, a premium is placed on getting private businesses to police themselves. That was the rationale for new guidance from the Departments of Commerce, Treasury, and Justice published in July 2023 in the form of a **Tri-Seal Compliance Note**. The Note highlighted new changes to DOJ's voluntary self-disclosure policy, provided an overview of recent changes to the Department of Commerce's voluntary self-disclosure policy, and generally highlighted the Department of Treasury's policy. The Note also discussed the potential monetary benefits associated with the Financial Crimes Enforcement Network (FinCEN) anti-money laundering and sanctions whistleblower program. While the Note did little to alter current policy, it signaled clearly that regulators very much want private businesses to voluntarily self-disclose violations, reiterating the array of benefits in place to those companies that disclose. Striking a common theme with other Biden administration guidance, the Tri-Seal Compliance Note stridently recommends that companies invest in strong compliance programs.

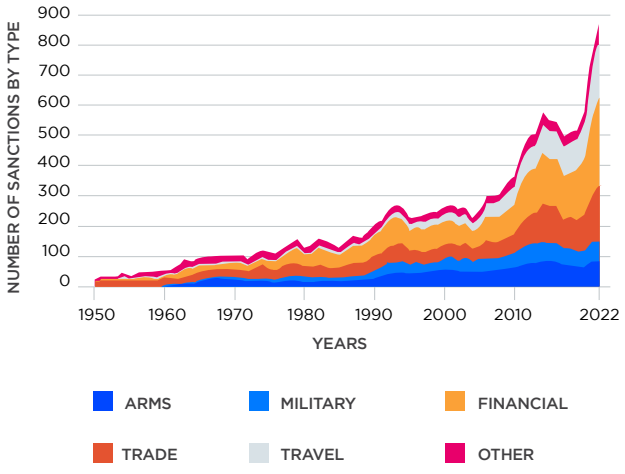
Know-Your-Customer/Business Diligence

Recent changes in U.S. trade law have elevated the importance of know-your-customer/business (KCY/B) practices. Not only are there many more restrictions on particular goods and entities, but the legal standard applied to suspected illicit goods has changed in some instances. For instance, the Uyghur Forced Labor Prevention Act (UFLPA) prohibits goods from being imported into the U. S that are either produced, in whole or in part, from goods in the Xinjiang region of China or produced by certain entities identified on the UFLPA Entity List, unless there is clear and convincing evidence that the goods were not produced with forced labor. As of August 1, 2023, over 1,700 UFLPA-linked shipments have been denied by U.S. Customs and Border Protection (CBP) with a value of over $1.7 billion. Industrial and manufacturing materials are the second-most detained category of goods, with over 400 shipments denied.

CBP has made it clear that transshipment concerns are being taken seriously. Transshipment—the practice of shipping goods to a final destination through an intermediate country—has been a strategy of those seeking to circumvent U.S. trade law, and UFLPA-related data reveal that goods directly imported from China represent a relatively small percentage of detained shipments. This enforcement approach highlights the need for companies to develop greater insight into their supply chains, especially considering the Kafkaesque fate of detained shipments that can languish in a kind of bureaucratic limbo for months on end.

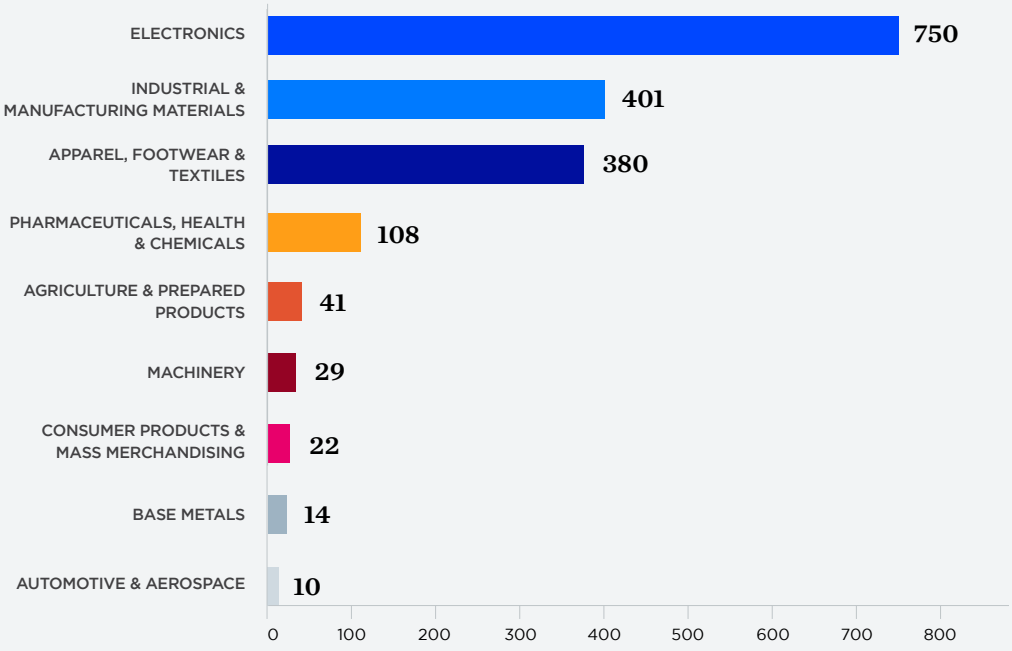
NUMBER AND TYPE OF SANCTIONS, 1950-2022





Source: T. Clifton Morgan, Constantinos Syropoulos, and Yoto V. Yotov, "Economic Sanctions: Evolution, Consequences, and Challenges," *Journal of Economic Perspectives*, Vol 37, No. 1 (Winter 2023)

UFLPA ENFORCEMENT: DETAINED SHIPMENTS BY INDUSTRY*



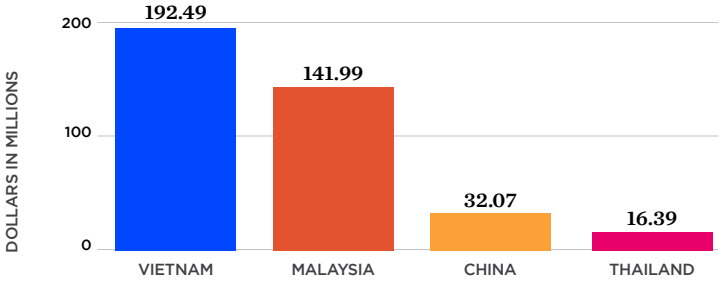
*From June FY2022 to August 1, 2023.

Source: U.S. Customs and Border Protection.

Clearly, companies that lack supply chain transparency risk major interruptions to their business operations, and UFLPA is only one source of that risk. The ongoing conflict between Russia and Ukraine has spawned numerous sanctions against Russian entities, but Russia has in some cases achieved a level of success in evading sanctions via transshipment of goods through other countries, such as China, Turkey, Hungary and the United Arab Emirates. In September 2023, the U.S. government expanded its export control net, sanctioning more than 150 foreign entities suspected of abetting Russian circumvention in an effort to cripple Russia's military supply chain.

Senior officials in the U.S. and EU have also hinted lately that their ability to track the transshipment of export-controlled goods bound for Russia has been greatly enhanced by new approaches to monitoring commerce, including the advanced use of tax data and other information that provides a nearer to real-time picture of how and where circumvention efforts are underway.

UFLPA ENFORCEMENT: VALUE OF DETAINED SHIPMENTS BY COUNTRY OF ORIGIN*



*From June FY2022 to August 1, 2023.

Source: U.S. Customs and Border Protection.

Cosmetics Manufacturing

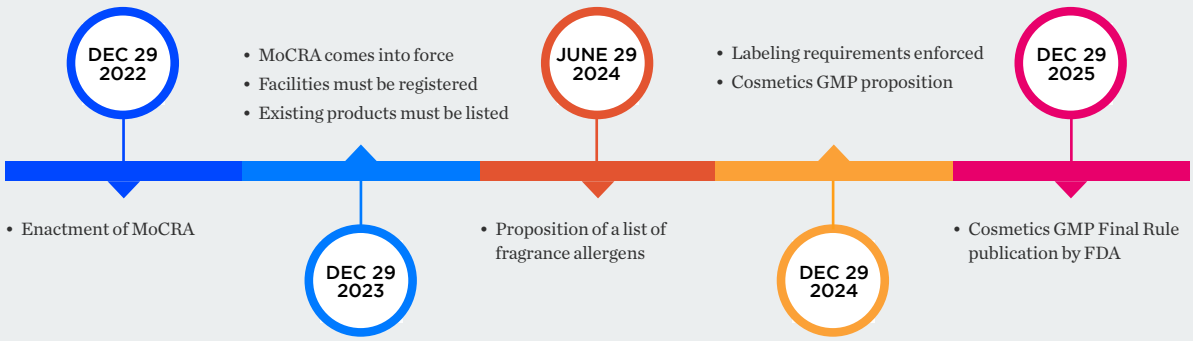
The Modernization of Cosmetics Regulation Act represents the first major change to U.S. cosmetics law since 1938, and the industry needs to prepare now for the FDA's vastly enhanced regulatory powers with respect to cosmetic products.

The Modernization of Cosmetics Regulation Act of 2022 (MoCRA) was signed into law on December 29, 2022, expanding the authority of the U.S. Food and Drug Administration (FDA) to regulate cosmetics and serving as the most significant change to the regulation of cosmetics since the passage of the Federal Food, Drug, and Cosmetic (FD&C) Act in 1938. MoCRA is a seismic shift in the world of cosmetic regulation, bringing new authorities to the FDA similar to those that currently exist for food, drugs, and medical devices, among other regulated products.

In the pre-MoCRA world, the FDA's enforcement authority over cosmetics was limited. Cosmetic products determined to be hazardous by the FDA required legal action through the FDA's seizure or injunction authorities, but manufacturers were not required to submit information to the FDA about production facilities, distribution chains, or product formulations. This left most cosmetic products unregulated, although the FDA had established the Voluntary Cosmetic Registration Program (VCRP) in 1972. The program was, as the name suggests, voluntary, and in March 2023, the FDA discontinued it in preparation for the MoCRA mandates. Even if a facility is already registered with the old VCRP, MoCRA will require it to be resubmitted for registration. Furthermore, there is little reason to believe that the information held within the VCRP will be transferred into a new system or how responsive that information will be within the context of the new regulatory mandates. In other words, it is likely that substantial compliance work lies ahead for the industry.

In September 2023 the FDA opened a **public comment period** for manufacturers to provide input on the FDA's newly developed draft electronic submission portal (Cosmetics Direct) and paper forms (Forms FDA 5066 and 5067).

MOCRA TIMELINE



Source: Cosmeservice

MOCRA COMPLIANCE: NEW MANDATORY REQUIREMENTS

THE RESPONSIBLE PERSON

The label of each cosmetic product must disclose the name and U.S. contact information of a "responsible person" (either the manufacturer, packer, or distributor of the product). The "responsible person" will serve as the point of contact for adverse event reporting and, among other duties, will be responsible for safety substantiation.

FRAGRANCE ALLERGENS

The cosmetic product labels will have to disclose "fragrance allergens," although details pertaining to what exactly will have to be disclosed are to be established by the FDA in 2024. This is expected to potentially implicate disclosure of information previously regarded as a trade secret, and it is bound to be the subject of vigorous public comment.

REGISTRATION AND LISTING

Each marketed cosmetic product, along with its ingredients, must be submitted to the FDA in an annual listing. Similar product listing systems exist for drugs and medical devices. Cosmetic manufacturing facilities will need to register with the FDA and update their facility registration every two years. The FDA now has the authority to withdraw a facility's registration where there is a reasonable probability that a cosmetic product poses serious adverse health consequences or death. This is similar to the food facility registration requirements. The FDA released its product listing and facility registration guidelines in August 2023 and will issue the final rule by December 29, 2023.

SAFETY SUBSTANTIATION

Cosmetic products manufacturers will be required to support any claims of safety of their products, and such support will be subject to the FDA's audit. Serious adverse events associated with the use of cosmetic products in the U.S. will have to be reported to the FDA. The FDA will have the authority to request access to records and issue mandatory recalls of cosmetic products. This record access authority for cosmetics is similar to other authorities granted to the FDA with respect to foods and drugs.

GOOD MANUFACTURING PRACTICES

The FDA will issue mandatory good manufacturing practices (GMPs) for cosmetic manufacturers. The GMPs are expected to be generally consistent with national and international standards.

TALC/PFAS

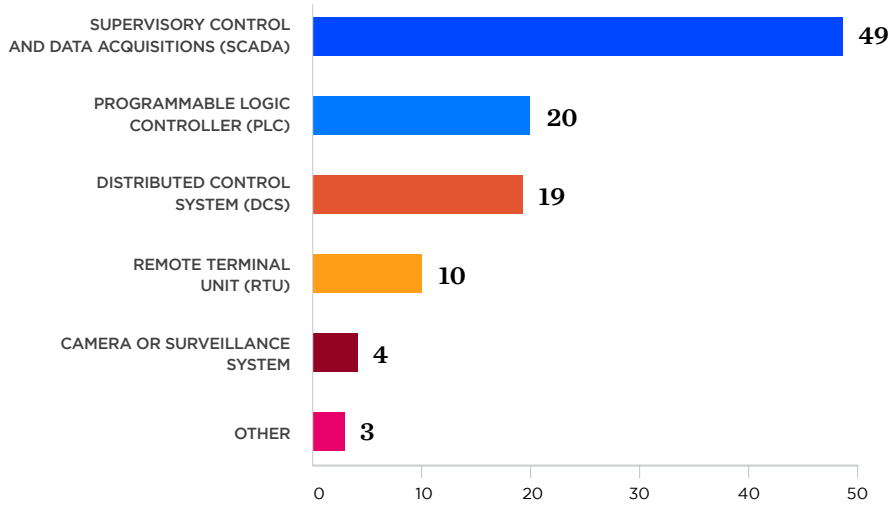
The FDA is also expected to issue rules pertaining to standard testing and detection methods for the purported presence of asbestos in talc and regulations pertaining to PFAS that may implicate preemption considerations in future litigation.

Cybersecurity

As threat actors and attack surfaces proliferate, the protection of data systems, proprietary information, and operational technology from malicious cyber activity continues to rate among manufacturers' top priorities.

Cybersecurity in the manufacturing industry continues to challenge corporate officers and directors, requiring evermore focus, planning, and expense. Digital technologies are quickly reconfiguring production processes and interfacing with the physical world in a complex web of analog machines and digital networks, such that the notion of cybersecurity has expanded beyond bits and bytes into the physical world, implicating individual enterprises and—when critical infrastructure is the target—the collective security of entire nations.

MOST FREQUENTLY TARGETED OPERATIONAL TECHNOLOGIES AND SYSTEMS*



*Study cohort included 122 international cybersecurity incidents affecting operational technology and integrated control systems.

Source: Rockwell Automation and Cyentia Institute, Anatomy of 100+ Cybersecurity Incidents in Industrial Operations.

For manufacturers, the cybersecurity challenge is two-fold. First, there are the enterprise-level issues that any company faces, where malicious actors attempt to gain access to networks and data in order to exercise control over the system, disrupt operations, and/or exfiltrate information. But cyber vulnerabilities for manufacturers extend beyond the architecture of corporate networks and into the supply chain. Components sourced from third parties used in the manufacturing process could be compromised; in turn, those components could find their way into the end product, creating a ripple effect of risk and liability. Thus, a manufacturer's enterprise-level risks can quickly become systemic, necessitating that manufacturers implement and maintain detailed, well-practiced incident response protocols.

SEC Implements New Cybersecurity Rules

Today is the perfect opportunity to review, revise, and supplement these incident response protocols in light of the Securities and Exchange Commission's (SEC) newly implemented cybersecurity rules and CISA's yet-to-be-released Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) regulations.

The SEC's new rules will greatly impact the manner and timing of how companies disclose cybersecurity incidents. The SEC purports that the new rules enhance and standardize registrants' cybersecurity risk management, strategy, governance, and incident response disclosures; however, given the Commission's limited perspective and its regulatory focus on investor protection and market operations, in practice the rules could create as many problems as they solve, especially for the critical manufacturing sector, whose scope of concern is necessarily far greater than securities law, and who will also have to comply with regulations promulgated under CIRCIA.

To the extent that the SEC has possibly jumped the gun with Congress's intent under CIRCIA and the White House's National Cybersecurity Strategy, hopefully the Office of the National Cyber Director will succeed in harmonizing the regulatory disparities and inconsistencies facing businesses in the critical infrastructure sectors.

One of the difficulties for manufacturers in complying with the new rules is the dissonance between the concept of materiality—central to securities law and public company accounting—and the practical, day-to-day operations of the manufacturing industry and its complex supply chains. This is clearly illustrated by the SEC's definition of "information systems." The final rules do not specifically mention or exclude operational technology (OT) systems. In fact, the adopting release confirms that the SEC "decline[s] to define operational technology as suggested by some commenters because the term does not appear in the rules we are adopting." While cybersecurity guidelines and best practices often focus on how cyber vulnerabilities can create problems in the physical world, it is useful to remember that physical or OT vulnerabilities can be used to create and exploit cyber vulnerabilities as well. This two-way risk sits awkwardly within the final rules, which raise as many questions as they answer regarding OT-related events.

COMPLIANCE TIMELINE FOR SEC CYBERSECURITY RULES

JULY 26, 2023	SEC adopts new cyber rules for U.S. and foreign issuers.
SEPTEMBER 5, 2023	Final rules go into effect.
DECEMBER 15, 2023	Annual reports must include disclosures regarding the companies' risk management, strategy, and governance structure to address cybersecurity risks (Item 106 of Regulation S-K). This means calendar-year reporting companies must comply with the new rules in their upcoming annual reports.
DECEMBER 18, 2023	All registrants other than "smaller reporting companies" must begin complying with the incident disclosure requirements (Item 1.05 of Form 8-K).
JUNE 15, 2024	Smaller reporting companies must begin complying with Item 1.05 of Form 8-K .

As a result, it is possible that Item 1.05 of Form 8-K could be triggered by a series of related occurrences that are each on their own immaterial but are deemed material in the aggregate. If factual circumstances drive this possibility, that outcome would ironically contradict the SEC's decision to omit from the materiality analysis the aggregation of immaterial incidents.

The final rules also complicate the question of where disclosure obligations can or should rest. Based on the definition of an "Information System" and the express language of Item 1.05, the SEC's clear preference is for the end user of an Information System to bear the disclosure burden, not the developer. This regulatory preference comes at a time when the executive branch, through the National Cybersecurity Strategy, is redirecting cybersecurity obligations to the companies best suited to defend the cyber ecosystem—the developers and internet service providers—and advocating for regulatory harmonization; however, the SEC has declined to get on board, choosing to place the reporting burden on the customers that purchase these Information Systems and the associated software and applications. Likewise, the SEC's inconsistencies created another risk to investors by ignoring the place of OT within the cybersecurity ecosystem. By excluding OT systems from the reporting requirements, the SEC did not reduce or eliminate the vulnerabilities that might exist in a registrant's OT systems, and material failures in these systems could have catastrophic results in the physical environment. In any event, registrants that own, operate, and use OT systems in addition to Information Systems should perform an asset inventory to document what devices and information are subject to the final rules and what devices and information are outside the rules' scope.

Due to the definitions at play, the new rules potentially misdirect the reporting obligations away from the actual source of the risk (product manufacturers and software developers) and onto the registrants that installed the product onto their information systems. It seems that the SEC's focus was on traditional data breaches where malicious actors can or do affect the confidentiality, integrity, or availability of company data, and less so on situations where software or hardware vulnerabilities are detected but the actor has yet to attack a company's information system.

For example, if the SEC's requirements had been in effect when the Orion, log4j, or MOVEit vulnerabilities were disclosed, only one of those developers would have been subject to the SEC's disclosure requirements. Instead, the reporting burden would have fallen on the registrants who installed the products onto their systems and are subject to an SEC enforcement regime that protects investors, not the U. S. economy writ large.

All of these concerns weigh heavily on the teams tasked with evaluating cybersecurity events and incidents, determining whether the incident escalation criteria have been triggered, and preparing routine SEC disclosures and crafting the protocols for disclosing material cybersecurity incidents within the mandated timeline. Not only must they develop the substantive basis for such disclosures, but they also need to make sure the full range of stakeholders are involved in their development and that the same processes are documented for cybersecurity incidents that are determined to be non-material, as the new rules have raised the stakes considerably for making those determinations. Any public regulatory disclosure—and SEC filings are no different—provides government enforcement efforts and potential private plaintiffs with a lot of information to consider. The same could be said for cybercriminals, who doubtlessly will be perusing the SEC disclosures with an eye toward spotting vulnerabilities in companies' security architectures. These factors must be weighed against the need to make good-faith efforts at compliance.

SEC Definition of "Information Systems"

Per the addition of Item 106 to Regulation S-K, the final SEC cybersecurity rules define Information Systems to be:

- the electronic information resources, owned or used by the registrant,
- including physical or virtual infrastructure controlled by such information resources, or components thereof,
- organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of the registrant's information to maintain or support the registrant's operations.

Encoded at 17 CFR § 229.106.

(Limited) Exceptions to the Rules

The requirement that public companies report material cybersecurity incidents to the SEC within four days is subject to two narrow exceptions, one of which could be hugely consequential to manufacturers. If the U.S. Attorney General (AG) determines that disclosing the material cybersecurity incident poses a substantial risk to national security or public safety and notifies the SEC of that determination in writing, the disclosure may be delayed for an initial period of up to 30 days, which can be extended for additional periods in certain circumstances.

The SEC rejected a multitude of suggestions from public commenters to accept extensions granted by other law enforcement entities or the regulatory agencies with responsibility for various industry sectors, or so-called Sector Risk Management Agencies (SRMAs). Instead, the adopting release notes that the AG is free to take into consideration other federal or law enforcement agencies' findings, but from a practical standpoint, such interagency coordination is highly unlikely to be completed in the four business days after a company determines an incident was material. [1]

In the absence of contrary guidance from the FBI in the future, companies should strongly consider utilizing SRMAs (in additional to the local FBI field office) to assist in efforts to expedite interagency coordination if they believe a cybersecurity incident might pose a risk to national security or public safety. Such coordination could be vital in contacting the AG's office and beginning the coordination process if an extension might be needed. As an adjunct to this approach, companies—particularly those in or adjacent to critical infrastructure sectors—should seek to develop good working relationships with relevant FBI field offices or SRMAs before an incident occurs.

[1]DOJ is taking steps to overcome this challenge. In August 2023 the FBI updated its cybercrime website to inform the public that the FBI is working with DOJ to develop additional guidance for the private sector on the intake and evaluation process for such requests. The FBI will update their website as the guidance is developed.

New SEC Cybersecurity Requirements

New Form 8-K Item 1.05 will require registrants to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations.

Registrants must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file an Item 1.05 Form 8-K generally within four business days of such determination. The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. If the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through possible exemptive orders.

New Regulation S-K Item 106 will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant. Item 106 will also require registrants to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Form 6-K will be amended to require foreign private issuers to furnish information on material cybersecurity incidents that they make or are required to make public or otherwise disclose in a foreign jurisdiction to any stock exchange or to security holders. Form 20-F will be amended to require that foreign private issuers make periodic disclosure comparable to that required in new Regulation S-K Item 106.

Source: U.S. Securities and Exchange Commission, **"Fact Sheet: Public Company Cybersecurity Disclosures; Final Rules"**

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.

Given the potential difficulties and time considerations in seeking an exemption, companies should identify events that will trigger secondary consequences or additional compliance requirements as part of their tabletop exercises and planning processes. For example, the disclosure of a material cybersecurity incident within four business days of the materiality determination most likely will precede the data breach notices that must be sent to individuals (and potentially effected business partners, customers, and clients) and the applicable state attorneys general offices. This type of disclosure may spark an influx of attention from external stakeholders before corporate leaders have a chance to allocate the resources needed to support customer service teams. The same disclosure will likely prompt plaintiffs' attorneys and class action advocates to commence litigation based on the Form 8-K disclosure before the full scope of the incident is known. It will be ironic if the legacy of the SEC's four-day deadline becomes premature corporate disclosures, followed by an influx of premature lawsuits, that result in a waste of corporate resources—all to the detriment of the investors the SEC seeks to protect.

SPOTLIGHT ISSUE

Artificial Intelligence

Excitement over the potential of AI has manufacturers scrambling to prepare and issue policies that address employee use of AI in a work setting, especially from the standpoint of intellectual property law.

Artificial intelligence is everywhere and continues to be an "ask for forgiveness later" model of use in many cases. The potential legal issues range from privacy concerns to employment issues related to discrimination in the AI algorithms. One looming area that implicates the core of a company's strategic advantage, intellectual property (IP), is changing every day. The three main buckets of IP—patent, copyright, and trademark—each have nuanced issues that should be considered before a company uses AI, especially in connection with the use of open-source software.

Patents

For once, the patent system seems decently positioned to address cutting-edge technology like AI. More specifically, protecting inventions that use AI and underlying training modules have been, and seemingly will continue to be, protectable under the standard *Alice* framework that is used to determine patent eligibility for software related inventions, so long as the AI invention meets the *Alice* test. A more difficult question arises as to who owns an invention that is made by AI. Currently, the U.S. Patent and Trademark Office and the courts have said that only humans can be an inventor. At this point, a company risks not being able to protect an invention generated by AI via the patent system, so there should be caution when AI is being used to invent something new.

Trademarks

Trademark law is an area of IP that is currently agnostic as to who (or what?) created the trademark because trademark rights are established by use. If a company is using a trademark generated by AI, it should be aware that the underlying AI system may not be reviewing the AI trademark against existing and potentially confusingly similar trademarks. After all—and by definition—AI is generating a new trademark and leveraging existing marks in its training modules.

Thomson Reuters v. Ross: A Case Worth Watching

A potentially seminal case is working its way through the federal court system involving the unauthorized use of data and/or content to train AI systems.

In September 2023, a federal judge **largely denied summary judgment to both parties**, setting up a potential jury trial at an undetermined date in the future.

Fundamental to the case are questions involving fair use. If the defendant's fair use defense is found to be valid, it stands to reason that AI developers will increasingly turn to it to protect themselves against future copyright infringement claims.

(*Thomson Reuters Enterprise Centre GmbH et al. v. ROSS Intelligence Inc.*, 1:20-cv-00613, U.S. District Court for the District of Delaware.)

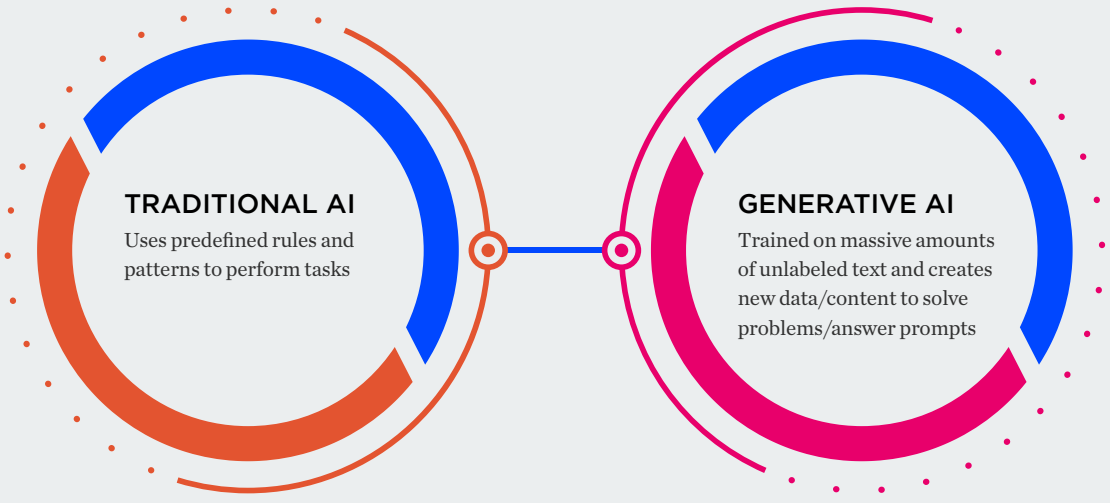
Copyright

Copyright is the most complex of IP areas that are implicated in AI. More specifically, copyright law allows a copyright creator to have exclusive rights to reproduce/copy their works and creative derivative works. Both areas are implicated in AI. First, the genesis of AI is training the models based on existing data sets. This training necessarily involves copying data that is owned by someone else and using it to train the AI system. The copyright/training aspect of AI is the dispute in numerous recently filed copyright infringement cases that are currently pending. In short, content creators have not given their permission for AI companies to use their data/content to train their AI systems. Second, the output of the AI creates an additional potential issue. More specifically, the output of the AI system may be considered a derivative work of the underlying original document or source(s). Because ownership of derivative works belongs to the original copyright holder, there is a question as to how this output can be legally used by a company.

Open-Source Software

Finally, there is an additional issue surrounding the use of AI-based systems to generate software code. The legal landscape of the generation of software code has already been complicated by the rise of viral open-source licenses including AGPL and GPL, but the intersection of open-source software and AI creates a new complexity. In particular, open-source software is being used to train some of the AI systems that are being used to generate code. Outside of the potential copyright issues, some open-source software licenses may 'infect" the output code just by virtue of the AI training on the code. Additionally, the output of the AI-based code generator may include some or all code that is subject to open-source restrictions. The current rubric does not allow for an end user to easily discern if open-source software has been used in the output code and potentially subjects a business to severe penalties for not complying with the licenses.

Ultimately, the use of AI has enormous potential to enhance the R&D efforts of a company, but there also continues to be risk-management challenges associated with commercializing the output of AI.



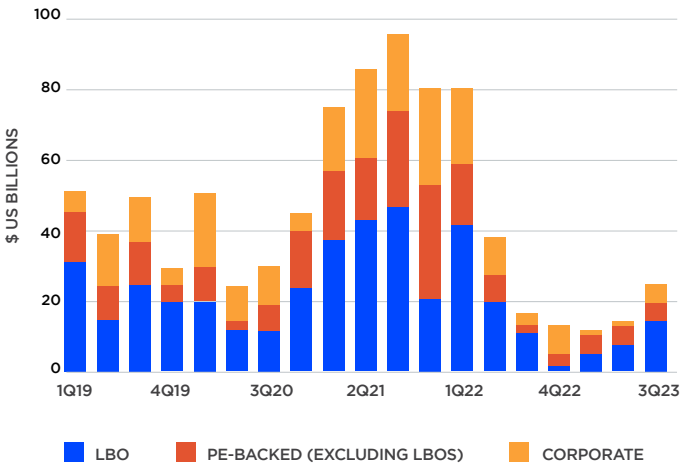
Corporate Transactions

Many of the factors in play at the beginning of 2023—such as higher interest rates and low levels of business confidence—have continued to suppress corporate megadeals, although some sectors of the manufacturing industry have defied the trends.

Through the first half of 2023, global mergers and acquisitions declined markedly from prior years, experiencing a 17 percent decrease in volume and a 40 percent decrease in aggregate deal value year over year; however, some segments of the U.S. manufacturing industry continue to get deals done. The current environment favors cash-rich companies seeking opportunistic transactions. With its substantial store of deployable capital, private equity continues to play a role as well.

Leveraged lending in support of M&A plummeted in 2022 and is expected to remain suppressed throughout 2023, given the current interest rate trajectory. Strategic buyers accounted for roughly half of the deal activity in the industrials and manufacturing sector, and the current set of circumstances should continue to help strategic buyers with cash on hand to deploy, as marginal buyers exit the deal space and the private equity secondary market continues to cool.

U.S. INSTITUTIONAL LOAN VOLUME BACKING M&A



Source: Pitchbook | LCD (Data through September 25, 2023)

2022 STRATEGIC BUYER DEAL PARTICIPATION

Selected Industrial & Manufacturing Sectors

	STRATEGIC BUYER MARKET SHARE		OVERALL 2022 DEAL STATISTICS	
	PUBLIC %	PRIVATE %	DEAL VOLUME	YOY CHANGE (%)
CHEMICALS/PLASTICS	29.1	35.6	289	-25.1
ENVIRONMENTAL, HEALTH & SAFETY	9.0	36.0	186	-13.9
HVAC EQUIPMENT & SERVICES	9.2	32.3	229	18.7
INDUSTRIAL PACKAGING	9.0	36.0	172	-11.8
PRECISION MANUFACTURING	9.0	36.0	195	-9.3
WASTE & RECYCLING	29.7	31.8	296	25.4

Source: Capstone Partners, Industrials Industry Middle Market Deal Activity & Outlook 2023, April 18, 2023.

Newly Proposed HSR Rules and Merger Guidelines

Dealmaking has slowed, but the pace of the U.S. government's regulation of mergers and acquisitions has not. Consistent with the Biden administration's whole-of-government approach to address perceived consolidation in a variety of industries, the Federal Trade Commission (FTC) and DOJ Antitrust Division are continuing to make good on their promise to increase scrutiny of mergers and acquisitions through newly proposed rules and revised merger guidelines.

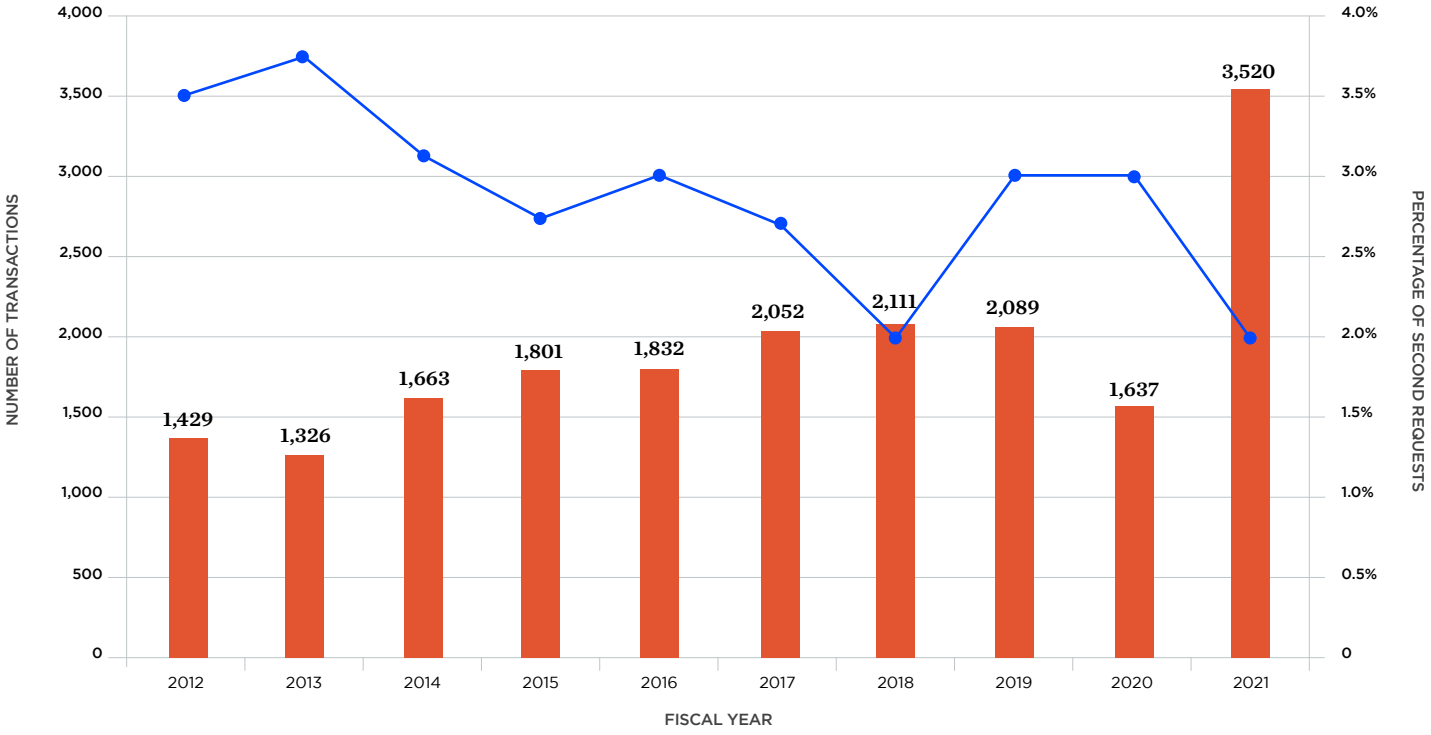
The agencies jointly published their draft **Merger Guidelines** on July 19, 2023, just weeks after the FTC issued newly proposed rules under the Hart-Scott-Rodino Antitrust Improvements Act of 1976 (HSR). The new draft Merger Guidelines represent a significant departure from the 2010 Horizontal and Vertical Merger Guidelines, and the recently proposed HSR rules represent the first time the HSR process has been substantively updated in over 40 years. If implemented in their current form, both will have the effect of making the merger review process lengthier, more complicated, and more burdensome. The public comment window on these items closed in September 2023.

Key takeaways from the draft Merger Guidelines include:

- Decrease in market concentration threshold used to evaluate whether a transaction presumptively violates antitrust law
- Increased focus on vertical mergers and increased likelihood that many different types of vertical transactions may be reviewed
- Continued efforts by DOJ and FTC to review mergers for effects on workers and labor markets
- Private equity acquisitions and rollups are specifically mentioned in the Merger Guidelines

Prior to the publication of these proposed guidelines, the FTC proposed its updated HSR rules. Given that the proposed HSR rules require more information from the parties, it is expected that the additional information could result in longer reviews and an increased number of formal investigations, but the most recently available data on merger clearance suggest that,

REPORTED TRANSACTIONS UNDER HSR & PERCENTAGE OF SECOND REQUESTS



Source: Federal Trade Commission and Department of Justice, "Hart-Scott-Rodino Annual Report Fiscal Year 2021," www.ftc.gov/system/files/ftc_gov/pdf/p110014fy2021hsrannualreport.pdf

despite the heightened rhetoric and regulatory action from the administration, over 99 percent of reported deals clear HSR review.

The FTC's proposed HSR rules mirror some of the newly announced guidelines and will require HSR filers to submit additional or new information as follows:

- Areas of actual or potential competition, vertical supply relationships, and strategic rationale for the transaction
- Detailed information about the post-transaction structure and the parties' organization, including more information about minority interest holders
- Disclosure of both parties' acquisitions going back 10 years where there is horizontal overlap
- More expansive disclosure of HSR Item 4(c) and 4(d) documents, including those of supervising deal team leaders and drafts
- Disclosure of foreign entity or government subsidies
- Disclosure of labor market data

For companies evaluating M&A opportunities, the proposed HSR rules and the government's more complex Merger Guidelines will likely increase deal timelines, the merging parties' time and expense, and the potential risk that the transaction will be reviewed. While the rules are not yet in place, FTC and DOJ are already evaluating transactions with an eye towards labor market effects, dominance, and vertical concerns. Given that the agencies are using the draft guidelines in practice, companies and organizations should carefully consider risk-shifting provisions, the antitrust clearance strategy, their appetite to defend against a litigated merger challenge, possible remedies, and settlement options at the beginning of a proposed transaction.

SPOTLIGHT ISSUE

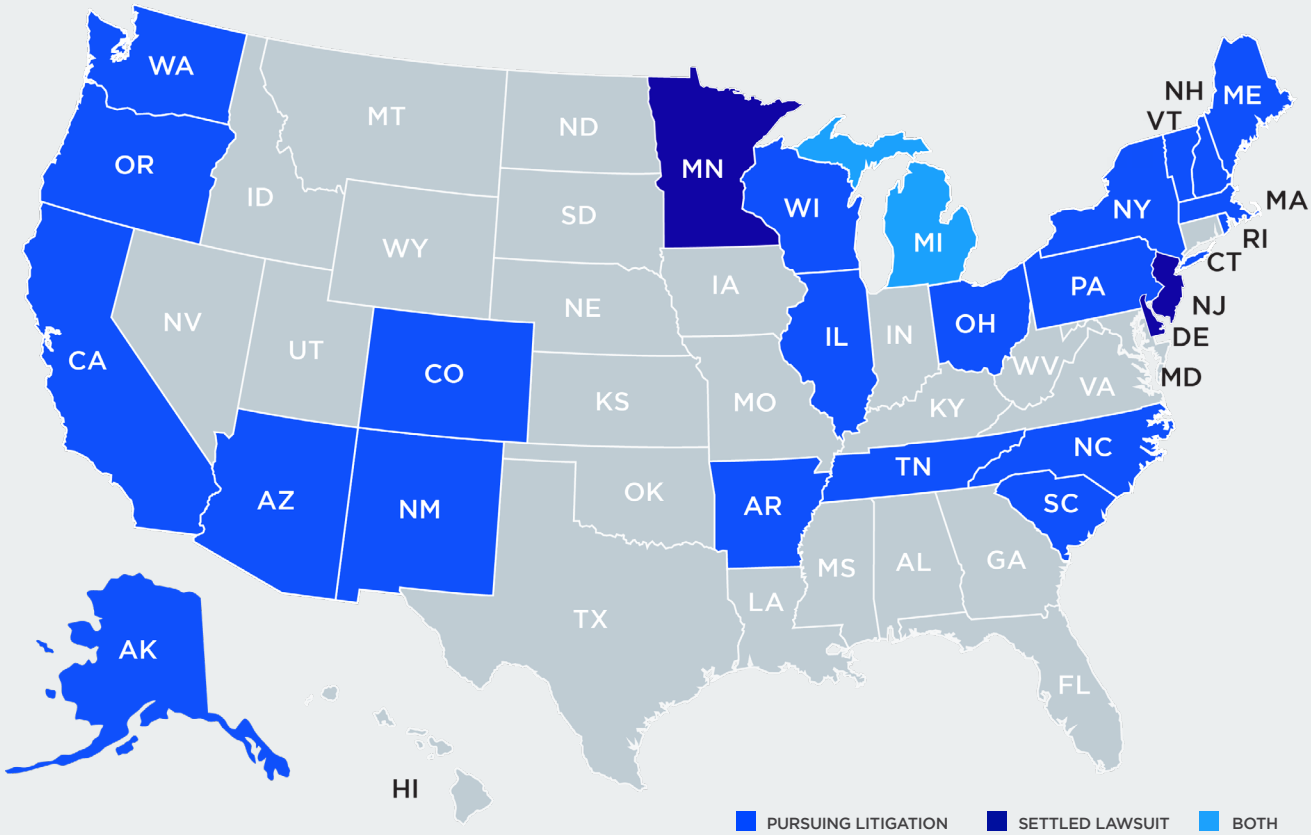
PFAS

The current and legacy use of PFAS in the manufacturing industry continues to generate potential legal liability as regulators and private litigants expand the scope of concern regarding these chemicals.

The term PFAS represents a diverse family of substances comprising thousands of individual compounds having different physical properties and chemical profiles. First employed in the 1940s, certain PFAS compounds were found to be useful because they possess a variety of properties, including non-flammability, heat conductivity, low surface tension, hydrophobicity, and resistance to degradation in oil, water, and heat.

Recently, as analytical testing has improved, certain PFAS substances exhibiting this resistance to degradation have garnered attention by regulators in the context of their trace detection in the environment and their relative persistence. While the science surrounding this class of chemicals is still evolving, legal settlements are moving forward; already, major manufacturers have entered into settlements totaling approximately **$12 billion as of mid-2023.**

STATE ATTORNEY GENERAL PFAS LAWSUITS



Source: Safer States, "More than half of US State Attorneys General have taken action against PFAS manufacturers and key users," August 24, 2023.

State attorneys general have been particularly active in initiating legal action concerning PFAS. As of the end of August 2023, 27 states have brought litigation against chemical manufacturers. These states are literally all over the map, covering every region of the country, and the state AGs bringing lawsuits are members of both major political parties. In July 2023 a group of state AGs had initially blocked a major settlement between one manufacturer and public water systems but later removed their objection following changes in the settlement's parameters. Those changes included a provision that locks in monies received by public water systems, regardless of the outcome of lawsuits involving other parties. These PFAS settlements have been the defining development for 2023 from a litigation standpoint. It is important, however, to bear in mind that they are tentative and are subject to the approval of the federal trial judge in charge of the massive multidistrict litigation (MDL) into which around 5,000 cases have been consolidated, a number which has grown substantially over time.

"What We Don't Fully Understand Yet"

Last updated in April 2023, EPA maintains a webpage titled **"PFAS Explained"** that explores what we know and don't know concerning PFAS, suggesting that the science behind PFAS is still very much evolving. The items EPA lists under "What We Don't Fully Understand Yet" include:

- How to better and more efficiently detect and measure PFAS in our air, water, soil, and fish and wildlife
- How much people are exposed to PFAS
- How harmful PFAS are to people and the environment
- How to remove PFAS from drinking water
- How to manage and dispose of PFAS

EPA Regulatory Developments

The Environmental Protection Agency (EPA) has been very active throughout the past 12 months in developing new approaches to PFAS regulation, particularly those utilizing the Toxic Substances Control Act (TSCA). In January 2023 EPA proposed a significant new use rule (SNUR) for hundreds of "inactive" PFAS, that is, those that have not been manufactured, imported, or processed in the U.S. since 2006 and are not already subject to a SNUR. The SNUR would require covered entities to provide EPA a Significant New Use Notice (SNUN) at least 90 days before resuming use of a covered chemical and gain its approval to move forward (EPA also proposed doubling the fees associated with submitting SNUNs to $45,000 per submission in November 2022). This proposed rule comes on the heels of a blitz of TSCA-related activity in late 2022. EPA proposed SNURs for 35 PFAS already subject to TSCA in December 2022. During the same month, the agency proposed adding certain PFAS to the list of Chemicals of Special Concern.

In April 2023, the EPA also sought to use the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), the so-called Superfund law, to designate certain PFAS chemicals as hazardous substances. This move creates an added layer of complexity to risk assessment, as the proposal would invoke the CERCLA framework for cleanup liabilities.

But far and away the highest profile move by EPA has been its proposed rules concerning levels of certain PFAS in drinking water, the first legally enforceable drinking water standards proposed for PFAS at the federal level. The proposed rules were forwarded in March 2023 and would regulate certain PFAS as contaminants subject to the agency's MCL enforcement framework under the Safe Drinking Water Act (SDWA). This involves monitoring, public notification, and treatment of water contaminated above the MCL guidelines. The proposed rules prompted over 120,000 public comments and will likely be finalized during the first quarter of 2024.

The projected costs associated with enforcement of the proposed rules vary but are thought to be potentially quite extensive, particularly for the public water systems tasked with real-world policy implementation. How the rules might impact manufacturers is uncertain, but the rules can be viewed as another possible source of expanding liability, especially given that the EPA's MCL framework will likely be pressed into service as a guideline for active and

future cleanup sites. The new rules' PFAS MCLs have been characterized by industry participants as very strict; at four parts per trillion for PFOA and PFOS, it is the lowest level that a laboratory can actually measure. SDWA mandates that EPA has 18 months to finalize the rules from the date of its announcement.

State Regulation of PFAS in Products

Since 2018, many state legislatures enacted bills to regulate PFAS in products, including firefighting foam, drinking water, food packaging, and other consumer products, while other state efforts focused on allocating money for remediation or requiring landfills to treat leachate for PFAS. The limitations on PFAS in consumer products, however, has been less than uniform. Of course, many states focused on firefighting foam as an early target, especially given its wide use directly into the environment.

Some states have expanded these early efforts to limit PFAS to other products. For instance, New York enacted a law that went into effect December 31, 2022, banning the use of PFAS in paper plates, cups, bowls, and other food packaging. Maine enacted a bill banning the use of PFAS in nonessential items and requiring the disclosure of PFAS in products to its Department of Environmental Protection beginning in 2023. This approach, like many states, is phased in over time, focusing on certain products first and then addressing others based on their contact with people or food, with the aim of banning PFAS use in all products by 2030. Similarly, in addition to its earlier bans enacted in recent years, California has also banned intentionally added PFAS from new juvenile products, beginning July 1, 2023, and banned the use of certain PFAS chemicals in cosmetics and baby clothing, both beginning January 1, 2025.

As the summary of legislative efforts above demonstrates, the number of states with bans of PFAS in products continues to grow in an inconsistent patchwork from state to state. Part of the confusion stems from a lack of scientific consensus regarding the substances themselves, and some state legislatures have rushed into this void with regulations that are untethered to the way PFAS are used, their prevalence, and their known or suspected impacts on public health. This tendency to view all substances in the PFAS category in the same light could lead to overbroad regulations that are inconsistently applied.

The unsettled nature of PFAS regulation and liability will likely have broad knock-on effects—both in the context of legacy and current PFAS usage—implicating a variety of areas, including supply chains and commercial contracts, international trade, and insurance coverage, among other things. Manufacturers will need to be proactive in managing these risks and develop tools that both allow them to stay compliant in a rapidly changing regulatory landscape and to prepare for an expected litigation onslaught for the past use of such products.

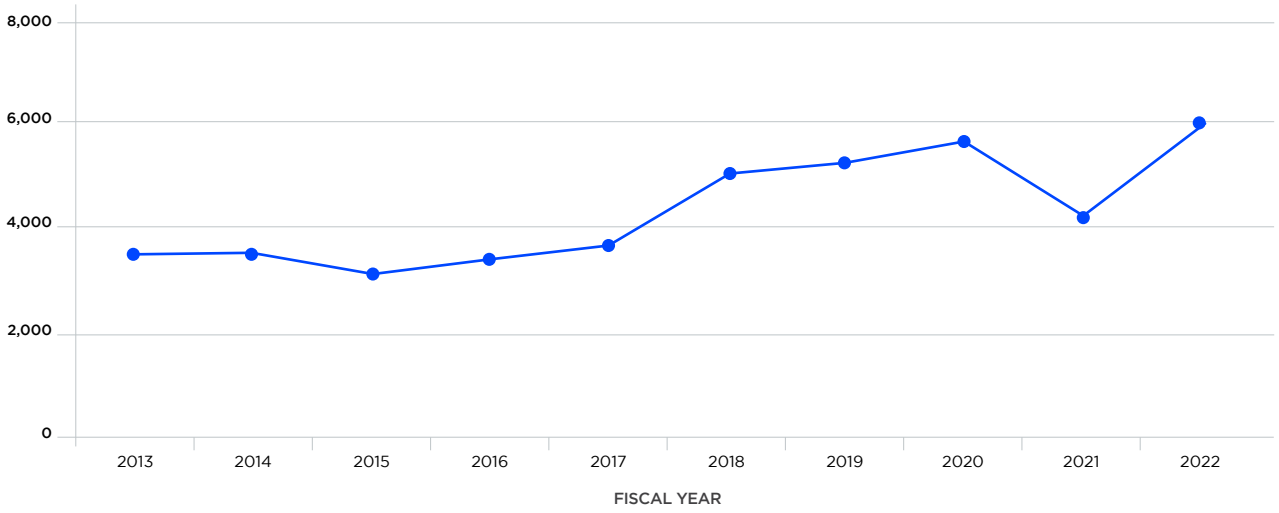
Product Liability, Safety & Marketing

Legal liability associated with alleged product defects continues to mount, as regulators turn to novel and aggressive tactics that could create higher levels of risk in the future.

As we anticipated in last year's report, product liability lawsuits shot up last year to record highs and show no signs of waning over the coming year. As we move further into the post-Covid era, there are several trends pushing product liability litigation to higher levels. Chief among these are skyrocketing jury verdicts, greater pools of litigation funding responding to these verdicts, and a growing sophistication by plaintiff firms in the way they research and target products and market themselves to potential claimants.

This rise in lawsuits parallels an increased number of product recalls. According to insurance technology firm Sedgwick, the first half of 2023 had **the most recall events for a half-year since 2011**. Similarly, the number of units impacted is on track to reach a six-year high in the consumer products segment, and overall, will likely eclipse one billion units once again in 2023.

PRODUCT LIABILITY CASES FILED, 2013-2022*



*Excluding MDL-associated cases.

Source: Lex Machina, 2023 Product Liability Litigation Report.

But the spike in recalls is only part of the broader enforcement story. Of late, the Consumer Products Safety Commission (CPSC) has demonstrated a notable willingness to use tools granted by Congress that exacerbate reputational and litigation risks faced by manufacturers. CPSC has always had statutory authority to effectuate product recalls and the filing of administrative complaints. As currently comprised, though, CPSC has expanded its use of so-called unilateral press releases that warn consumers about an alleged hazard associated with a product. From 2011 to 2019, CPSC issued two such press releases. Last year alone, the Commission issued no fewer than eight.

While the statutory tools available to the CPSC are significant, manufacturers can take some degree of solace in the law's due-process protections; however, by avoiding the procedures of a formal recall, the use of unilateral press releases creates unique vulnerabilities. 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.

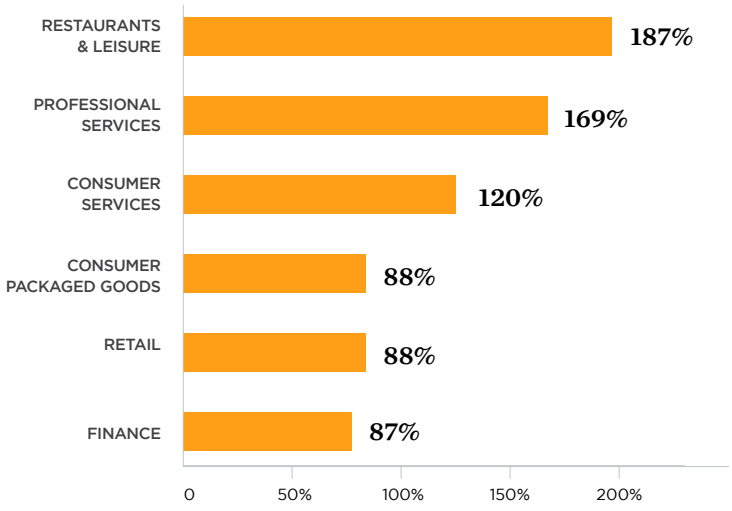
Consumer-Facing Digital Communications

The use of digital communications continues to be an area of great interest to manufacturers, both in terms of disseminating product safety information and product labeling and marketing. Covid-19 did much in the U.S. to resuscitate the usage and popularity of digital communications, particularly QR codes, those matrix barcode graphics that many service industries relied upon during the pandemic to promote social distancing. Likewise, the use of QR codes that link to product manuals and safety information has evolved quickly over the past few years and has thrown off interesting legal, regulatory, and operational questions for the manufacturers that employ this method of communication.

In response to the growing use of QR codes and other digital media, there has been a push to develop new industry standards and revise existing standards to guide businesses with their consumer-facing communications. Currently, the American National Standards Institute (ANSI) is contemplating a significant revision/addition of its safety signage and communication standards, found in **ANSI series Z535**. Currently under development is a new sub-standard, ANSI Z535.7, which is expected to cover certain electronic media—including videos, dynamic webpages, and virtual reality—however, existing sub-standards, in particular ANSI Z535.6, can be applied to many examples of printable, digitized communications in use by manufacturers. While ANSI standards have no official legal sanction, there is ample evidence that making good-faith efforts to incorporate these standards into consumer-facing communications can have a positive impact in the litigation context. Manufacturers should consult these standards when developing communications, particularly those focused on product safety and use information, and should pay attention to the new ANSI Z535.7 standards when they are finalized and made available.

YEAR-OVER-YEAR GROWTH OF GLOBAL QR CODE CREATIONS BY INDUSTRY

H1 2022 to H1 2023



Source: Bitly 2023 QR Code Trends Report

Greenwashing Class Actions: An Emerging Risk

As consumers increasingly seek out products with high sustainability ratings—and as investors continue to pour capital into ESG-themed investments—companies have been pressed to engage with this sentiment in their product marketing, highlighting the "green" features of their products. Predictably, this has led some marketing departments to push the envelope in promoting their products, and because the terms of art in this so-called green marketing can be fuzzy at best, there are disputes about how to define certain terms and concepts or how to use them in a marketing context, leading to allegations of "greenwashing"—the practice of overstating or misstating the environmental soundness of a product or company.

Manufacturers should be alert to the litigation risks in this form of consumer-facing communication, especially as regulators scramble to provide guidance and workable definitions. Take, for instance, the Federal Trade Commission (FTC) Green Guides, first issued in 1992 to guide companies' marketing statements about the environmental benefits of its goods and services. The Guides were last updated over a decade ago and have failed to respond to the evolving ESG movement, even as other agencies, such as the Securities and Exchange Commission, forward rules concerning investor communications and disclosures. The FTC requested public comment in December 2022 as to whether the Guides should be retained, modified, or withdrawn altogether. The comment window closed in April 2023.

While important in its own right as a major potential change in federal regulation, an update to the Green Guides would also have a significant impact on state-court litigation involving greenwashing. Several state consumer protection laws incorporate the Green Guides, and early examples of greenwashing lawsuits—there have been well over a dozen filed since July 2021—often rely on existing state consumer protection laws.

Compliance professionals will need to follow how the FTC rulemaking proceeds from here, as well as the arc of ongoing greenwashing class actions, and then develop programs and training for marketing and other communications professionals that manage risks associated with consumer-facing media.

2023 Legal Insights for Manufacturing Editorial Team

Wendy Arends
Partner | Madison
608.258.7382
wendy.arends@huschblackwell.com

Nicole Bashor
Partner | Chicago
312.526.1635
nicole.bashor@huschblackwell.com

Erik Dullea
Partner | Denver
303.749.7270
erik.dullea@huschblackwell.com

Thomas Godar
Of Counsel | Madison
608.234.6064
thomas.godar@huschblackwell.com

Sal Hernandez
Senior Compliance & Ethics Advisor | St. Louis
314.345.6193
sal.hernandez@huschblackwell.com

Trecia Moore
Senior Counsel | Kansas City
816.983.8260
trecia.moore@huschblackwell.com

Cortney Morgan
Partner | Washington, DC
202.378.2389
cortney.morgan@huschblackwell.com

Brandan Mueller
Partner | The Link
314.480.1825
brandan.mueller@huschblackwell.com

Magda Patitsas
Partner | The Link
202.378.2326
magda.patitsas@huschblackwell.com

Terry Potter
Senior Counsel | St. Louis
314.345.6438
terry.potter@huschblackwell.com

Kirstin Salzman
Partner | Kansas City
816.983.8316
kirstin.salzman@huschblackwell.com

Dominique Savinelli
Partner | The Link
312.526.1518
dominique.savinelli@huschblackwell.com

Jeffrey Sigmund
Partner | The Link
314.480.1834
jeffrey.sigmund@huschblackwell.com

Gregg Sofer
Partner | Austin
202.378.2383
gregg.sofer@huschblackwell.com

Please visit online Husch Blackwell's Manufacturing team page to view our entire team.