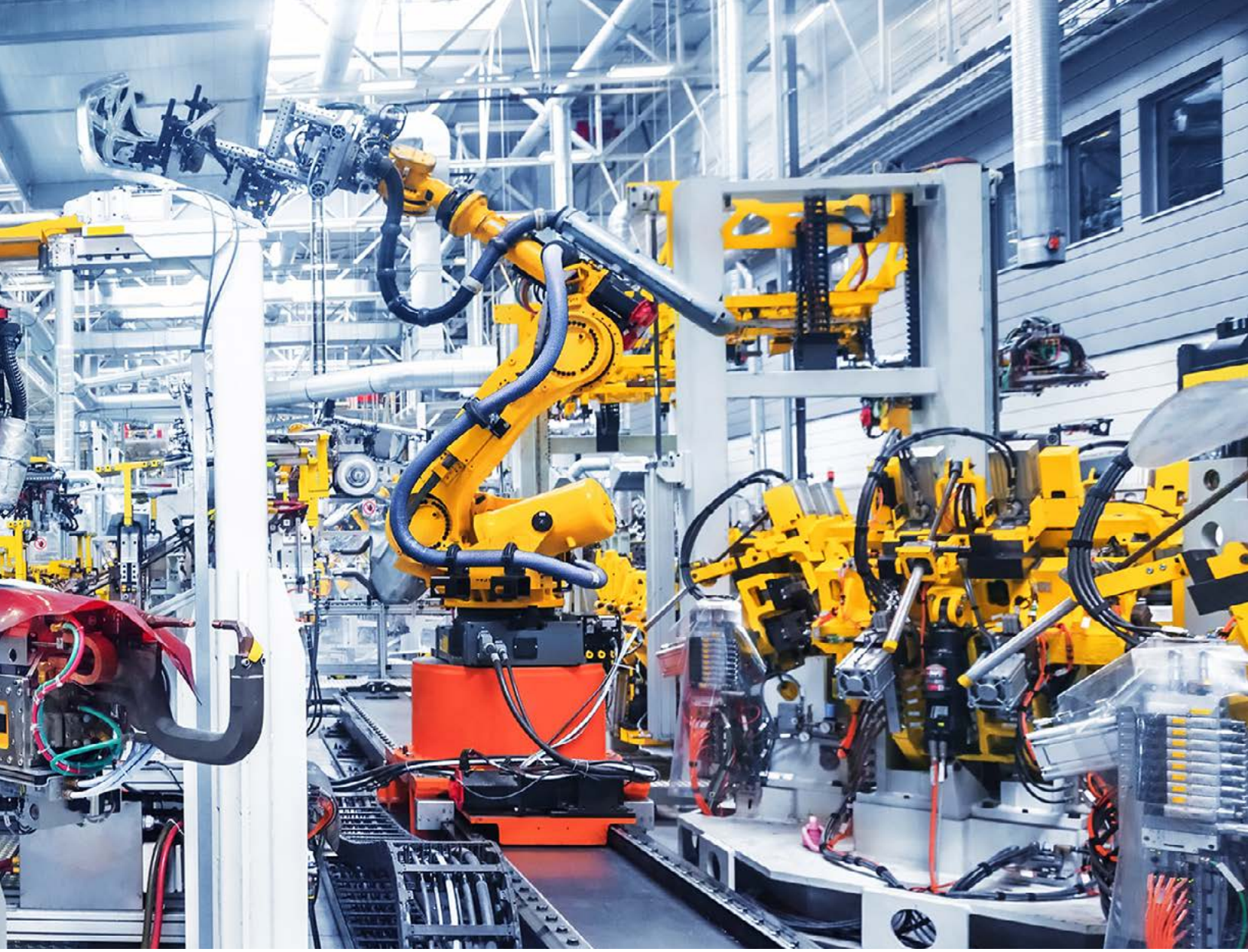


HUSCH BLACKWELL

LEGAL INSIGHTS FOR MANUFACTURING

A look ahead at the issues that will shape 2023 for the manufacturing industry

January 2023

INTRODUCTION

The manufacturing industry is entering a period of rapid reconfiguration, driven by the complex interaction of technological, geopolitical, macroeconomic, and financial factors.

The long-term trends that have shaped international commerce during the post-Cold War period are changing. The engines of the era—the relatively free flow of capital across borders, the lengthy and complex global supply chains, the super-cycle of cheap credit, the stable supply of energy, and the steadily liberalizing global trade regime—have stalled or reversed course, as we enter a new period defined by very different trends, including the reappearance of high inflation and a new appreciation for credit risk.

Our new report, *Legal Insights for Manufacturing*, explores how the legal and regulatory framework is evolving—and will evolve—to address the large generational shifts taking place. Broadly, these changes will potentially create risk in the following areas during 2023:

- Supply chain risk & reshoring
- Cybersecurity & data protection
- Heightened regulatory & enforcement risk
- Product safety & associated liability
- Increased unionization & skilled labor scarcity

These areas are not mutually exclusive, but rather overlap and reinforce each other. For example, supply chain disruptions create scarcity for key inputs, reinforcing global inflation as buyers bid up existing supply, and as we have seen in the recent past, entire production lines hang on the supply of key inputs—from electricity to semiconductor chips—that are less than stable due to a variety of factors. Additionally, as businesses seek out new suppliers, there is added risk relating to third-party compliance that touches on a number of regulatory concerns.

The choices made during this era of transition will be crucial, even existential, for many U.S. manufacturers. As companies continue to tackle the risks and opportunities in this challenging environment, we hope the framework presented here will help manufacturing leaders think creatively about the future and their way forward.

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

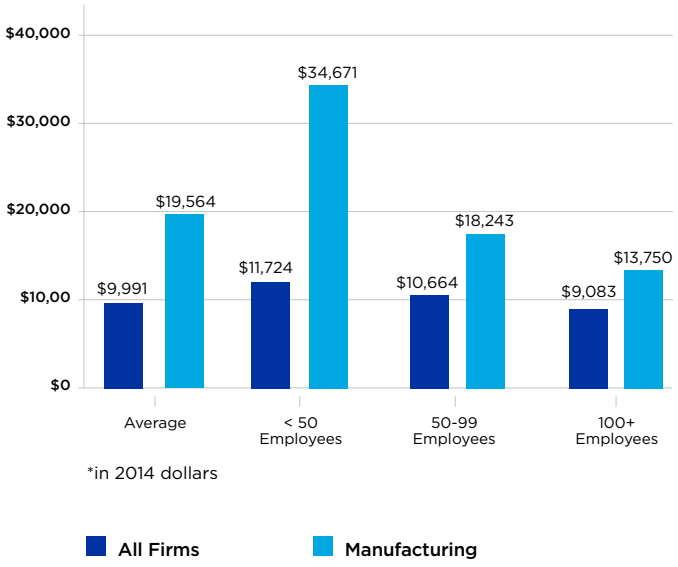
REGULATORY & COMPLIANCE

To say that businesses today face increasing risk and costs associated with government regulation is one of those statements that would appear to be perennially true; however, it will be particularly apt in 2023 for U.S. manufacturers.

Conventional wisdom suggests that the cost of regulatory compliance—and the volume of government enforcement actions—are headed well north of current levels on an across-the-board basis. From securities law and alleged Foreign Corrupt Practices Act (FCPA) violations to newly emergent Environment, Social & Governance (ESG) guidelines, those who expect greater regulation seem validated in the number of challenges that U.S. manufacturers grapple with every day.

In 2014, the National Association of Manufacturers published a landmark study revealing the costs associated with U.S. regulatory compliance for the manufacturing industry. The report illustrated what manufacturers long knew: making things in the U.S. carries with it a higher cost per employee than other industries; furthermore, that cost increases dramatically for smaller manufacturers that lack economies of scale.

Regulatory Cost per Employee*



Source: *National Association of Manufacturers*

In the decade since the NAM report debuted, the underlying economics associated with regulatory compliance have not improved by most measures. If anything, government officials have clearly signaled that enforcement—particularly of white collar crime—is going to be greater than in the recent past, requiring greater compliance costs to contain risk.

There has also been a steady rise in the criminalization of regulatory infractions. For example, the Department of Justice (DOJ) and Federal Trade Commission have recently pursued "naked wage-fixing [and] no-poach agreements" with criminal felony charges. Additionally, we are seeing greater across-the-board DOJ involvement in what were once mere regulatory enforcement actions.

Deputy Attorney General Lisa Monaco remarked in October 2021 that the DOJ is changing its approach to the enforcement of corporate crime and introduced three new initiatives—with the promise of additional changes in the works—that will significantly impact the way U.S. businesses view regulatory compliance and handle government criminal enforcement actions.

COOPERATION

Going forward corporations must name ALL individuals "involved in or responsible" for misconduct—not just those "substantially involved"—in order to receive credit for cooperating with investigations.

PRIOR MISCONDUCT

DOJ will direct its prosecutors to consider all prior misconduct at a corporation—no matter whether the misconduct was civil, regulatory, criminal and/or unrelated in any way to the situation under investigation—in evaluating resolutions related to current misconduct.

CORPORATE MONITORS

DOJ rescinded any guidance (to the extent it existed) that corporate monitors are disfavored.

The intent of these initiatives could not be clearer in signaling to U.S. manufacturers a change in DOJ's approach to the enforcement of corporate compliance. First and foremost, the implementation of these initiatives will necessarily change the parameters of corporate compliance programs, as well as corporate strategy for resolving disputes with the government. Monaco underscored this point, stating that "companies need to actively review their compliance programs to ensure they adequately monitor for and remediate misconduct—or else it's going to cost them down the line."

The Importance of Corporate Compliance Programs

As DOJ hires on more professionals with a background in private-sector compliance programs, the standard is being raised: more and more scrutiny will be applied to the quality of these programs. Those that lack seriousness—evidenced by being understaffed, under-resourced, and/or disempowered—will earn no special consideration from DOJ if and when enforcement actions occur.

Companies that already have compliance programs should rigorously assess them against DOJ's new initiatives and its Evaluation of Corporate Compliance Programs (ECCP) framework to ensure that the programs are actually managing regulatory risk in an acceptable manner.

900

Number of new FBI agents hired focusing on corporate crime.

5,521

Individuals charged in 2021 by DOJ with white collar offenses, a 10 percent YOY increase.

Heightened Areas of Regulatory Risk for 2023

FINANCIAL & ACCOUNTING

There is a correlation between economic downturns and accounting irregularities, particularly within public companies pressured to meet their quarterly or annual financial metrics. Regulators are well aware of the connection and are on the lookout for revenue misstatements, channel stuffing, improper "pull-forwards," unrecorded expenses, and other financial statement fraud.

DATA STEWARDSHIP

DOJ has made clear through its policy guidance and recent hiring practices the importance of data stewardship for corporate compliance programs. Data preservation and monitoring must now address personal devices and third-party messaging platforms and include training on their use. In the cooperation context, prosecutors will evaluate whether businesses have policies that help to capture information from employee devices and platforms.

FOREIGN CORRUPT PRACTICES ACT

We anticipated a rise in FCPA enforcement after an unusually quiet 2021, and there has been a slight uptick in FCPA and FCPA-related enforcement actions in 2022. We look for this trend to gather strength in 2023, particularly where DOJ's FCPA Unit employs a "shotgun" approach of bringing non-FCPA charges—such as money laundering, mail and wire fraud, and tax violations—in addition to or instead of FCPA charges.

SUPPLY CHAIN & LOGISTICS

As manufacturers scramble to secure adequate inputs at reasonable prices, many companies will establish relationships with new suppliers and staffing agencies. It becomes hugely important to make sure the evolving supply chain is in compliance with the array of relevant laws, including child labor, forced labor, and bans on inputs from sanctioned countries and regions. Compliance programs need to have effective processes in place to manage third-party risk.

LABOR & EMPLOYMENT

Self-described as "the most pro-union, pro-worker administration of our lifetime," the Biden presidency has implemented measures that tilt the balance of power in favor of labor, including key labor appointments at NLRB, FLRA, and OSHA and broadly pro-labor executive orders on government contracting and unionization rules. The administration's unabashed support for unions has clouded the outlook for manufacturers already struggling with a labor shortage.

ESG & CLIMATE CHANGE

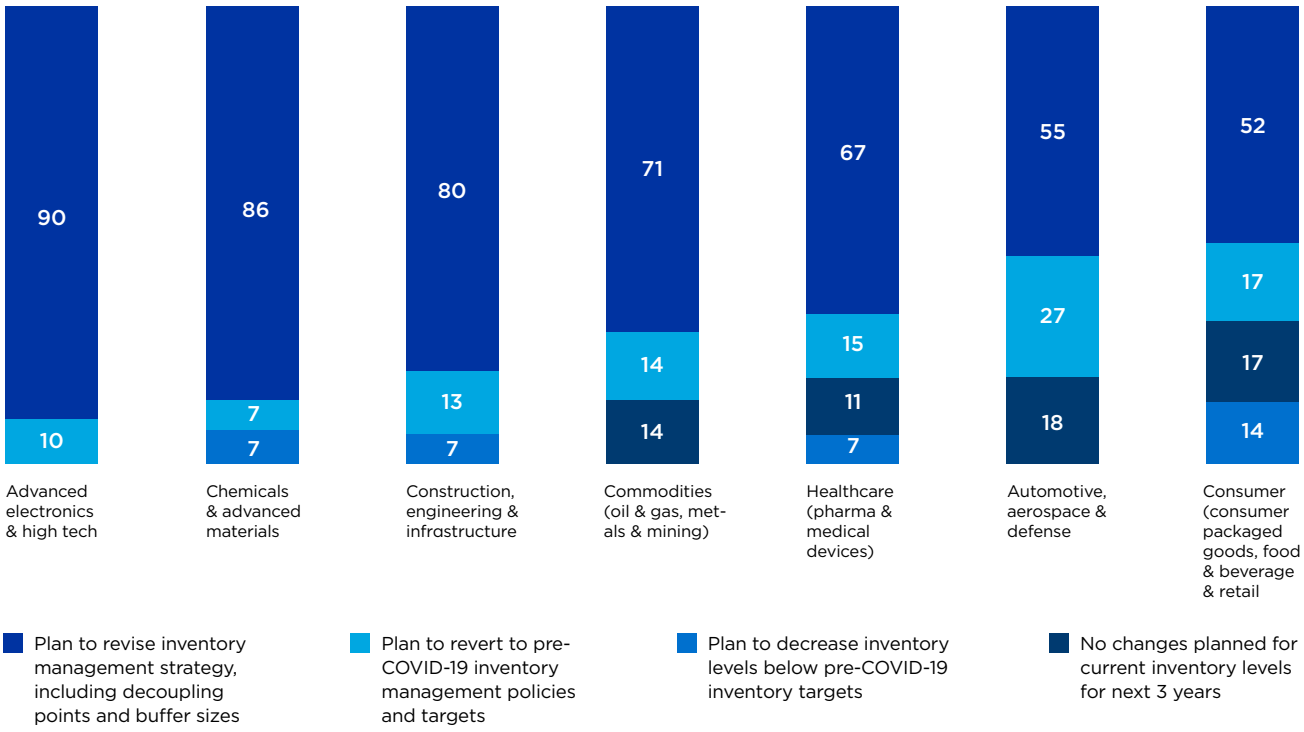
The rise of ESG has had a huge impact on capital allocation over the past few years, and come what may, that probably won't change in the near term. Companies need to act now to prepare for the raft of ESG-related disclosure obligations that are sure to follow, especially given the rise of "greenwashing" and other tactics that have allegedly misled investors regarding the ESG bona fides of companies and/or investment funds.

SUPPLY CHAIN & LOGISTICS

The onset of the global Covid pandemic inaugurated a new era of supply-chain vulnerability, product scarcity, and rampant inflation that has persisted well after the public health menace abated and that has upended business models predicated on just-in-time inventory and a relatively stable supply of key manufacturing inputs.

Recently conducted surveys of leaders across all sectors of manufacturing reveal a strong desire to rethink supply chain and inventory management, which is unsurprising given the experience of the past few years. The difficulty, of course, is in the implementation, as well as having shorter-term plans in place to manage the current dislocations.

Inventory Management Evolution over the Next 3 Years
% of respondents



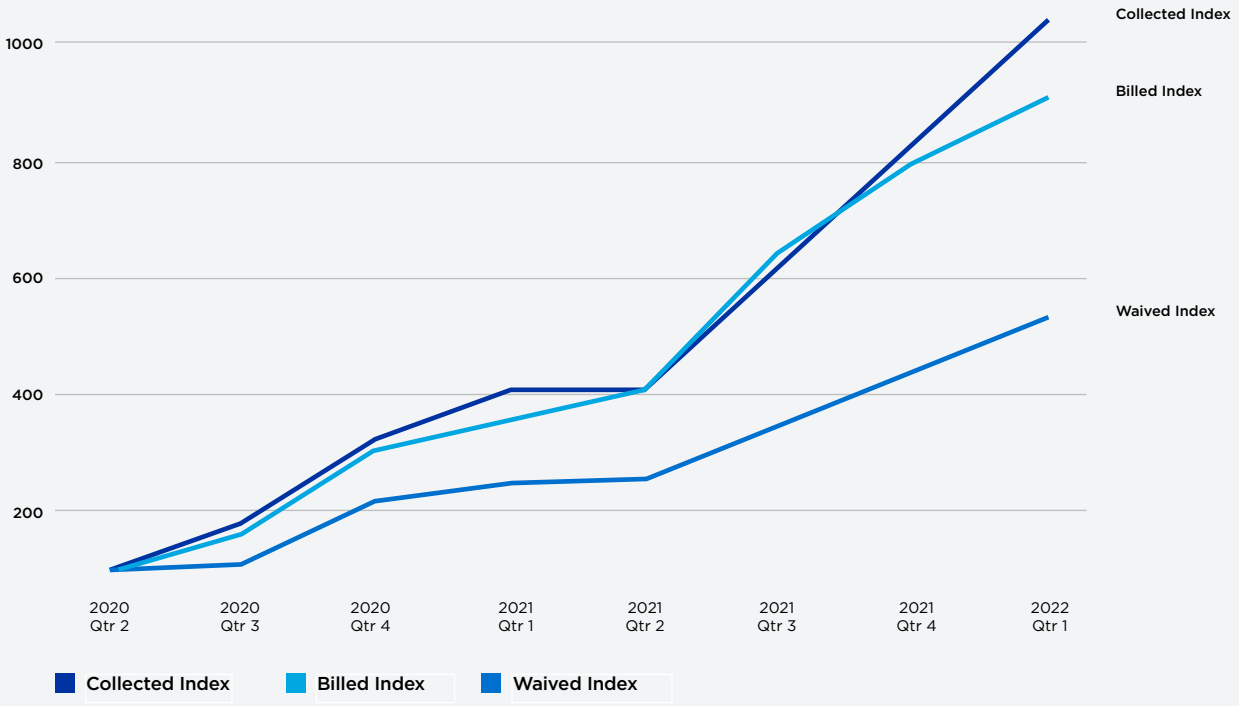
Source: *McKinsey & Company, "Taking the pulse of shifting supply chains," August 26, 2022*

Returning key supply chain links to North America is a popular notion, and only time will tell if it's more than a mere talking point or if the underlying economics make sense. For manufacturers unable to accomplish reshoring or nearshoring in a timely fashion, however, there is a possibility for improvement in the current logistical challenges in 2023. Port congestion continues to be the major impediment to the movement of goods internationally, as major U.S. ports are seeing import volumes running anywhere from 10 to 30 percent above pre-Covid levels; however, the number of ships waiting in offshore queues have fallen dramatically since the beginning of 2021 and shipping rates for containers have fallen throughout 2022.

Additionally, continuing economic weakness in the short term could lead to less import/export activity, taking stress off of the ports' capability to handle cargo.

Port congestion has spawned a web of legal issues. There has been a dramatic surge in the detention and demurrage (D&D) fees charged by carriers, and predictably, this has led to a significant increase in disputes, where shippers have been at a decided disadvantage. In June 2022 President Joseph Biden signed into law the Ocean Shipping Reform Act 2022, which accomplishes some significant burden-shifting in D&D disputes.

Detention and Demurrage Indices

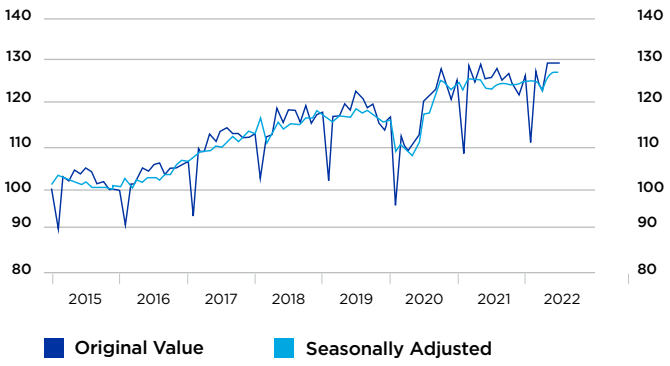


Source: *Federal Maritime Commission*

Among other things, ocean carriers now must provide accurate invoice information on D&D; failure to do so will result in refunds and penalties. The list of items that must be included in an invoice are those one would reasonably expect in terms of the facts that triggered the D&D, but they also must include contact information by which shippers can request mitigation of fees. Most importantly, the ocean carriers must provide statements that a) the charges are consistent with Federal Maritime Commission rules on D&D; and b) that the common carrier's performance did not cause or contribute to the underlying charges.

Port congestion is in some sense a result of greater volume and a lack of infrastructure, which puts stress on the entire system. These stresses inevitably lead to mistakes. For instance, the amount of cargo lost at sea spiked in 2020 and has remained elevated versus pre-Covid levels. The heightened risk of lost or damaged goods should occasion manufacturers to reevaluate their Incoterms 2020 contract review policies and procedures,

RWI/ISL Container Throughput Index
2015=100



Source: *RWI/ISL computations based on data provided by 94 ports, July 2022*

regardless of what segment of the supply chain is most relevant to their businesses. Risk profiles are changing, and terms that might have seemed acceptable last year could be very different in 2023, whether due to the underlying shipping risk or the insurance costs derived from these risks.

Supply Chain Agreements and IP Concerns

The current supply chain challenges highlight an increased need for top-to-bottom scrutiny of supplier relationships, including the intellectual property relationship between the parties. Manufacturers that have not pushed for IP ownership—or at least broad licenses—in these relationships are finding themselves in difficult positions and unable to swap out components freely. As a result, complex machines having thousands of components end up sitting on the factory floor unable to be shipped due to the sourcing requirements of a just a few components. At a minimum, manufacturers need to ensure that they are free to go to alternative suppliers in the event the current supplier cannot meet demand.

Ideally, a company can and should take a more proactive approach to ensure its own Background Intellectual Property is protected, both through the use of patent filings, as well as through the use of NDAs and other agreements. Additionally, a company should ensure that it is not disclosing confidential and proprietary information of a current supplier to a third party. This scenario can easily play out in this context where a company wants to see if a new supplier can "make this component." Finally, a company should ensure that it has Foreground Intellectual Property Rights in connection with the integration of the component into its system, use of the component in the system, and customized design requests related to the system, among other concerns, in the event a new supplier needs to be found.

INTERNATIONAL TRADE UPDATE

Last year, our team noted that the Trump-era trade policies might prove to be more lasting than some might have anticipated, a point was illustrated throughout 2022. Tariffs against Chinese imports continued, despite ongoing legal and lobbying efforts. 2022 has also brought increased scrutiny and enforcement by U.S. government agencies against importers for allegations of forced labor violations and potential evasion concerns relating to antidumping and countervailing duty orders currently in place. With Russia's invasion of Ukraine, U.S. companies are navigating a labyrinth of new export controls and sanctions against Russia, designated regions of Ukraine, and Belarus. We also saw new targeted sanctions against China, Colombia, Sudan and Venezuela. While the Biden administration has considered resuming talks with Iran concerning the Joint Comprehensive Plan of Action (JCPOA), Iran's recent support of Russia makes the lifting of any sanctions unlikely. We anticipate additional export controls on emerging technology, quantum computing and technology transfer will likely be released next year. Finally, U.S. companies engaged in international sales must stay alert to potential transshipment and diversion concerns in light of these new sanctions and export controls.

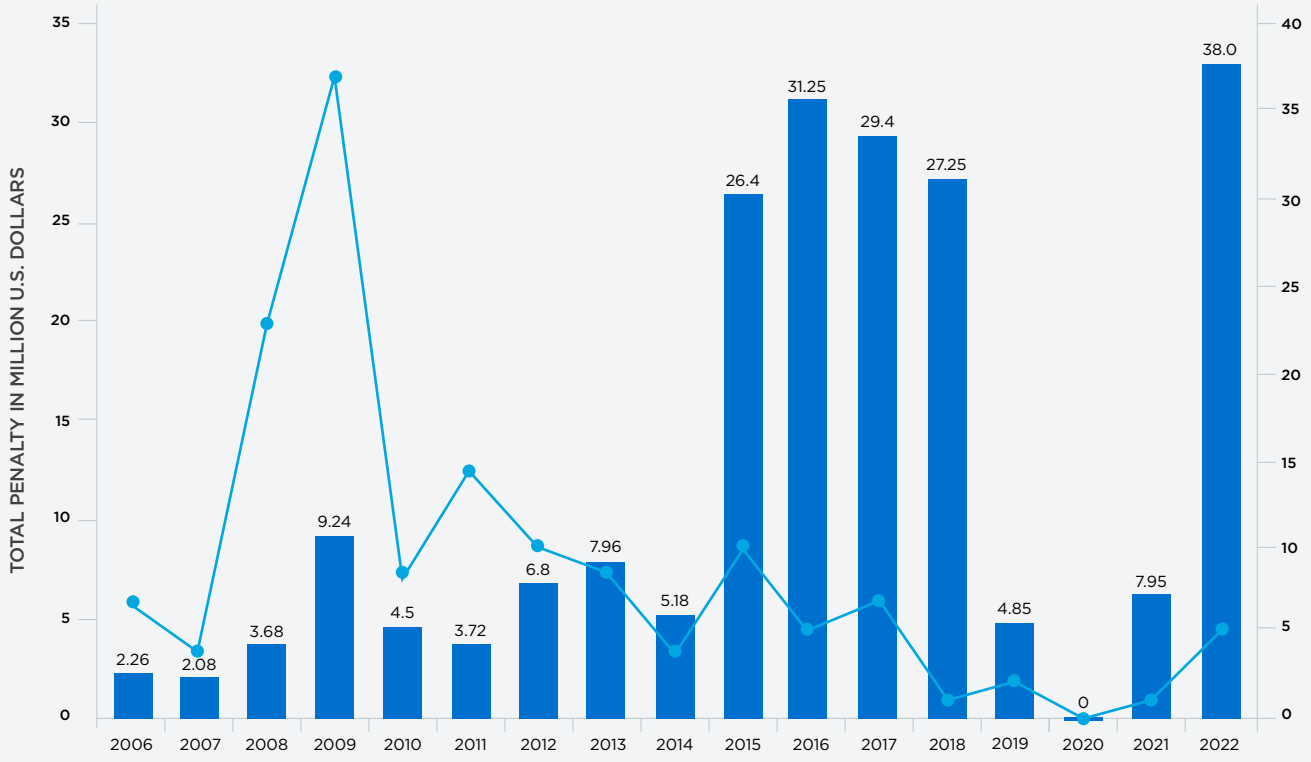
Refer to our International Trade Law Report, which published in late December, for more details.

Across the product lifecycle—from research and development to consumer marketing and liability disputes—manufacturers are being challenged by evolving regulatory standards, tighter enforcement, and novel theories of liability.

CPSC Reinvigorated

With a 45 percent budget increase and a three-to-two split favoring less business-friendly policies, the Consumer Product Safety Commission (CPSC) ramped up its enforcement activities in 2022 and pursued markedly higher civil penalties in conjunction with allegations of product defects. For manufacturers, the message is clear: expect greater levels of risk in bringing products to market. Through midyear 2022, CPSC recalls are on pace to exceed totals from recent years, but as 2021 demonstrated, the total number of recalls does not necessary capture the full picture. There were 25% fewer recalls in 2021, but three of them involved more than 100 million units. Overall, there were 1 billion recall-affected units in 2021. Similarly, after issuing just two civil penalties in 2021, CPSC doubled that total through the summer of 2022, with several sitting commissioners issuing after-the-fact statements about the inadequacy of the penalties, hinting that future penalties could be higher.

CPSC Civil Penalties, 2006-2022*

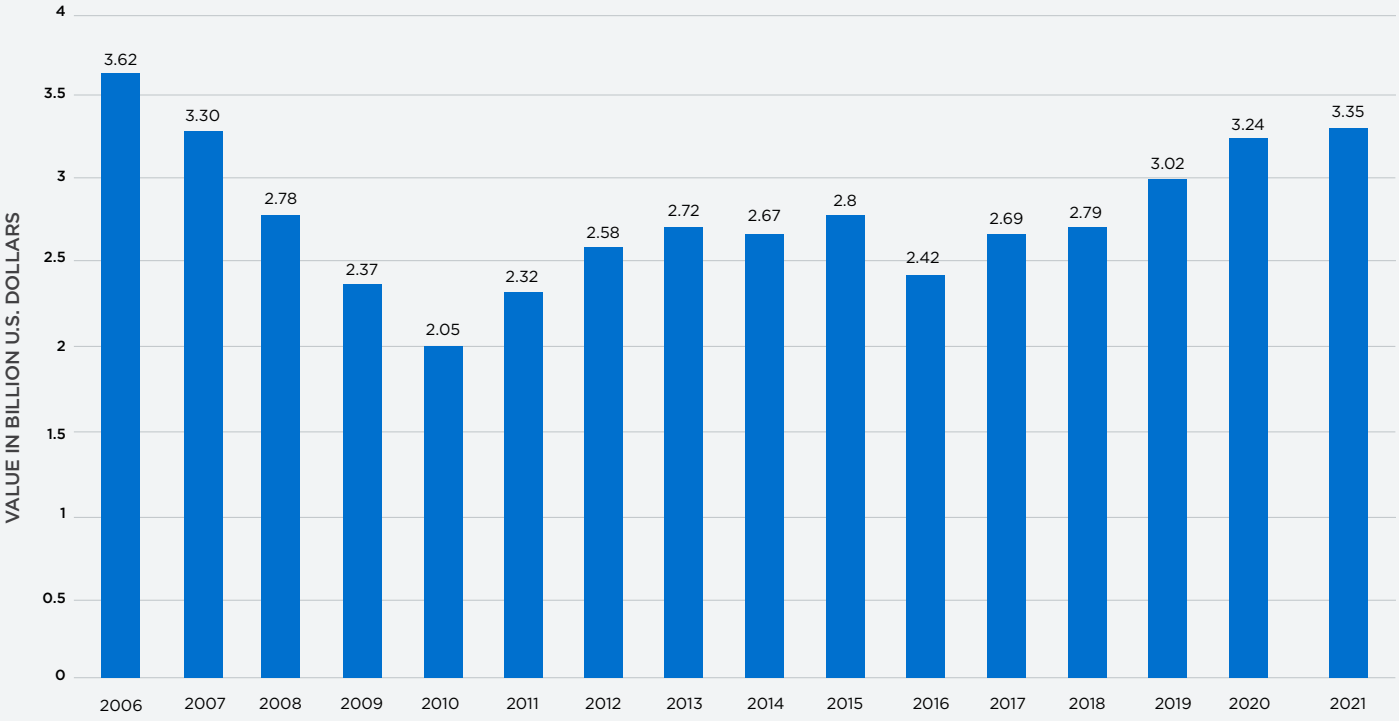


*2022 data are as of November 17, 2022

Source: *Consumer Product Safety Commision*

In a February 2022 statement, Commissioner Peter Feldman expounded upon a "Faster CPSC" approach, noting "I have long advocated that the Commission use its full complement of resources to protect American consumers. In my view, if a matter is serious enough for the Commission to issue a Health and Safety Finding to truncate the 6(b) process, it may be necessary to pair such public warnings with administrative litigation." Already, so-called unilateral safety announcements, once a rarity at the Commission, have been made at least six times since the beginning of 2021. Additionally, Congress continues to explore expanding CPSC's power to implement unilateral recalls. The prevalence of product-related risk, including the increase in the value of penalties and settlements, has led in part to the growth of product liability insurance in recent years, as risk gets priced—and repriced—in the marketplace.

U.S. Product Liability Insurance, Net Premiums*



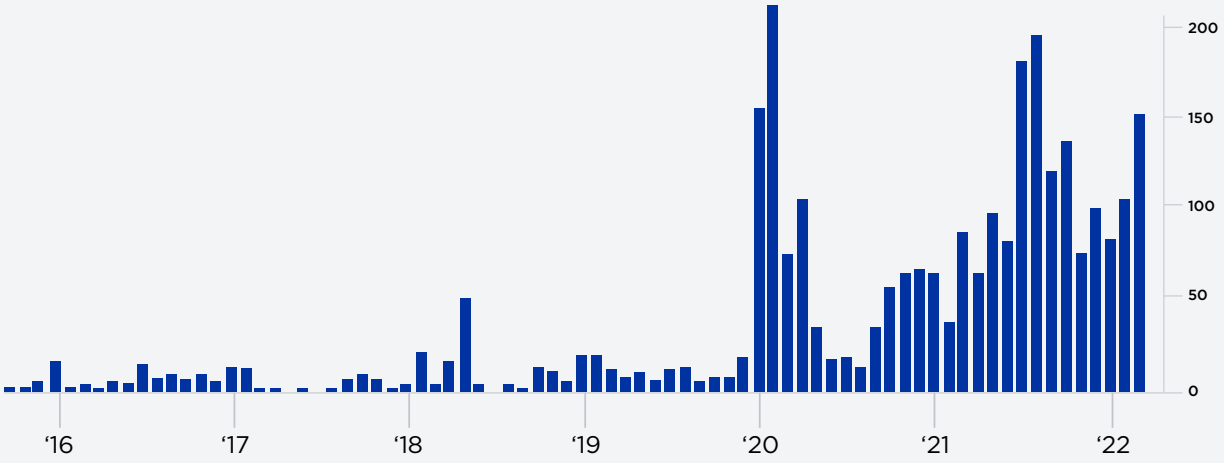
*After reinsurance transactions, excludes state funds

Source: *Insurance Information Institute*

Class Action Litigation Developments

As 2022 draws to a close, new developments in product-related class actions are occurring in multiple directions, three of which we note here. First, plaintiffs are targeting newer classes of chemicals and substances—most notably per- and polyfluoroalkyl substances, or PFAS—with traditional theories of liability. PFAS are often called "forever chemicals" because they do not naturally break down and studies suggest that they may be present in the blood of 97% of Americans. The plaintiffs' bar has aggressively targeted PFAS, applying to it an approach reminiscent of litigation involving polychlorinated biphenyls (PCBs) of the recent past, and the substances are the subject of a growing number of litigations across the country that forward a wide range of claims, including alleged property damage, violations of environmental law regulations, person injuries (cancer, etc.), calls for injunctive relief, and

Monthly PFAS Lawsuits Filed
October 2015 - March 2022



Source: *Bloomberg Law*

claims seeking the implementation of a medical monitoring fund. Products most at risk to PFAS litigation are those that used the substances for their waterproofing qualities and potentially include fast food containers, cookware, cosmetics, furniture, carpeting, waterproof clothing, electrical component insulation, personal protective equipment, and medical devices, among others. According to Bloomberg, some worst-case scenarios posit that total PFAS liabilities could reach as high as $30 billion.

At the federal level, there is currently a lack of comprehensive legislation governing PFAS; however, the past two Congresses have seen approximately 150 pieces of proposed legislation, according to the National Conference of State Legislatures. Also, the Infrastructure Investment and Jobs Act allocated $10 billion in new government funding to address PFAS and other emerging contaminants, including the distribution of $5 billion to address emerging contaminants under the Safe Drinking Water Act for small and disadvantaged communities; $1 billion for wastewater and stormwater infrastructure projects under the Clean Water State Revolving Funds (SRFs); and $4 billion for community water systems to upgrade drinking water treatment, distribution, and replacement of contaminated sources under the Drinking Water SRFs.

Given the lack of definitive federal legislation on PFAS, there is a patchwork of state laws and initiatives at work in the early PFAS litigation, and that patchwork has been in a constant state of flux. It is estimated that, as of September 2022, there are over 200 proposed bills in 31 states seeking to address PFAS. Notable recent efforts include California, where Governor Gavin Newsom signed Assembly Bill Nos. 1917 and 2771 into law on September 29, 2022. These statutes prohibit the manufacture, distribution, or sale of PFAS-containing textiles and cosmetic products respectively, effective January 1, 2025. In 2021, Maine passed a more sweeping law banning PFAS in all new products, but it does not come into effect until 2030. Other states such as Hawaii and Colorado have also passed laws banning the use of PFAS in specific product categories.

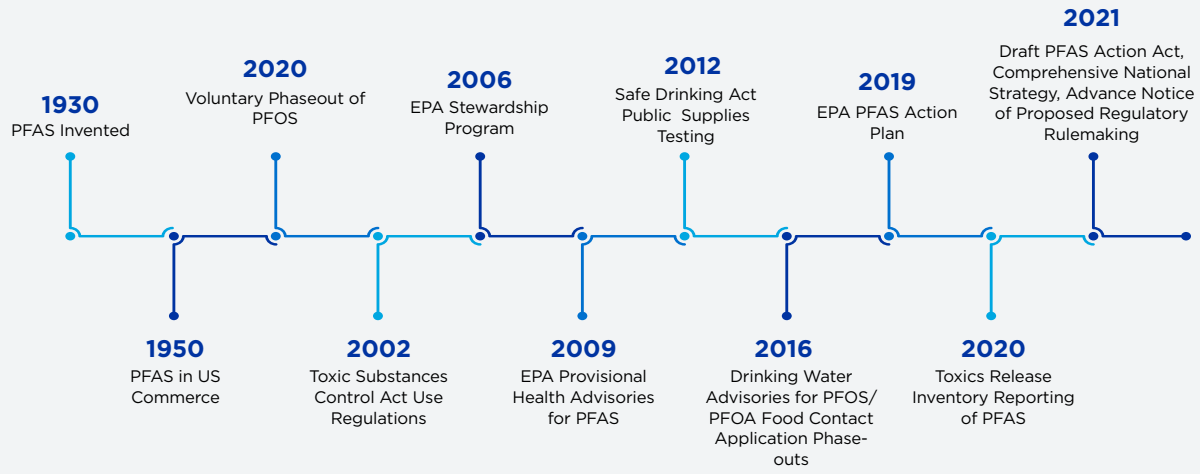
Additionally, the Environmental Protection Agency (EPA) has recently made news for increasing its regulation and tracking of PFAS. Last year, EPA issued UCMR 5, a rule which added 29 PFAS to the list of substances that community water systems must monitor under the Safe Drinking Water Act. More recently, EPA proposed amendments to the Toxic Control Substances Act (TSCA) which would require companies of all sizes to

retroactively report information regarding PFAS in their products. The proposed TSCA Section 8(A)(7) would require any company that imported, produced, or manufactured PFAS, or a product containing PFAS, since January 1, 2011, to report to EPA the specific types and quantities of the chemicals used, the manner in which the product and any byproducts were disposed of, the number of individuals exposed to these products and the duration of any such exposure, and information regarding each chemical's impact to the environment and human health. The bulk of this information, aside from certain trade secrets, will be made publicly available.

Aside from the staggering volume of information demanded (much of which will be difficult if not impossible for many companies to obtain), the proposed rule is also notable because there is no threshold triggering the reporting—that is, any company that imported or manufactured a single product over the last 12 years that contained any one of the thousands of PFAS chemicals would be subject to these requirements. There is no doubt that the publishing of these reports will spark a firestorm of new filings by plaintiffs' attorneys. The proposed rule is expected to be published by January 1, 2023.

As the profile of these lawsuits, agency rulemakings, and legislative efforts broadens, we anticipate greater attention from the plaintiffs' bar and a further spike in PFAS products-related litigation throughout 2023.

PFAS Timeline



A second area of note in products-related class action litigation involves the emergence of certain theories of liability, drawn from product liability law, but applied to nontangible "products," such as online platforms like social media websites. Websites that utilize user-created content have long been shielded from liability by Section 230 of the Communications Decency Act; however, plaintiffs are now seeking to evade these third-party publisher protections by claiming the platforms should be considered "products" subject to traditional claims of liability, such as design defects that harm users, especially children. While the targets of this novel approach are not manufacturers, any theory of liability that successfully expands the traditional notion of what a product is could have far-reaching unintended consequences and should be watched closely.

A third development worth noting—this time, a net positive one for manufacturers—is the rapid decline of so-called "no-injury" consumer class actions targeting alleged misstatements in product marketing, advertising and/or instructions for usage. In 2021, the U.S. Supreme Court vastly circumscribed the effectiveness of these claims, ruling in *TransUnion LLC v. Ramirez* that plaintiffs (including absent class members) must have suffered a concrete harm in order to have Article III standing to sue for damages. The decision on standing, however, only applies to federal lawsuits; it is possible that the "no-injury" class action strategy could become more a feature of plaintiffs pursuing federal statutory rights in state courts. Given the patchwork of approaches taken toward class action lawsuits at the state level, this could be good or bad for manufacturers, depending on the state.

Product Safety Communications

We continue to see disputes arise between manufacturers and consumers concerning the way product safety information is conveyed, particularly in the emerging use of digital communication formats, like QR codes and links to websites. There is also a complementary increase in the use of instructional videos and other digital visual media; however, there has been little in the way of firm guidance or regulation regarding the standards to be used in such communications. While its standards have no official legal sanction, the American National Standards Institute is due to release expanded guidance on digital communications before the end of 2022.

Given the relatively limitless scale of digital media as compared to printed manuals or on-product labeling, manufacturers could benefit greatly from the proper adoption and use of the newer digital communication formats. In consumer product liability litigation, much depends on the notion of adequacy, and in determining what is adequate, more is often better than less. Digital communication formats can help solve for this in conjunction with effective risk assessments at the outset of the product safety workflow.

Standard Product Safety Compliance Worflow for Manufacturing

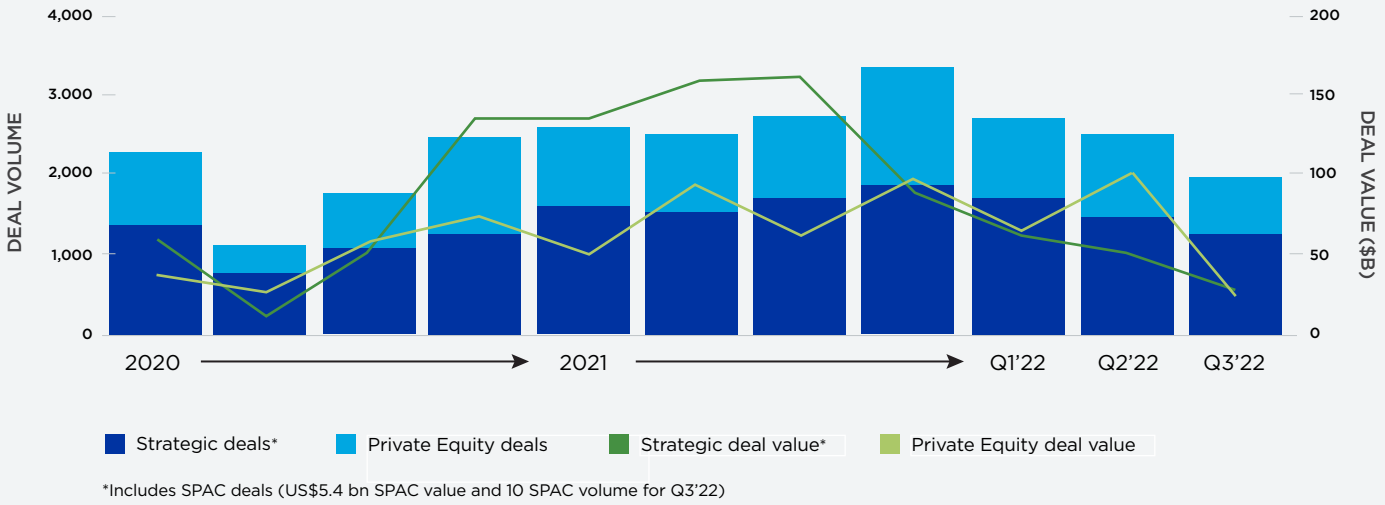
Integrating digital communication formats will present different risks as to the likelihood of misinterpretation by consumers and the ability of consumers who lack tech skills to access the information. Additionally, some industries—drug manufacturers come to mind—will find it harder to digitize given the array of regulations in place, but the added options available to product safety teams should be a net positive.

CORPORATE TRANSACTIONS

After peaking at the end of 2021, corporate dealmaking slowed considerably throughout 2022 as geopolitical uncertainty, a changing credit market cycle, and the threat of global economic contraction led to greater caution; however, the M&A market is still more active than pre-Covid levels, and generational shifts in manufacturing are creating opportunities for strategic acquisitions.

Strategic deal volumes declined from the 2021 highs but were still relatively strong, and the desire to acquire assets has not been shaken by the emerging challenges of the past year. Tellingly, only 19 percent of manufacturing industry leaders recently surveyed by KPMG, a global consultancy, anticipated a reduced appetite for M&A in the near term.

U.S. Manufacturing Industry M&A, 2020-2022



*Includes SPAC deals (US$5.4 bn SPAC value and 10 SPAC volume for Q3'22)

Source: KPMG, "Biding Time: M&A Trends in Industrial Manufacturing Q3 2022"

The larger concern for manufacturing executives is not a reluctance to buy assets, but rather integrating those assets post-transaction. Due diligence can often foreshadow post-transaction challenges, but emerging areas of risk have made the due diligence exercise much more complex as the number of tires to be kicked have increased, potentially increasing the complexity of deal negotiations and the potential for a failed transaction. For companies that seldom engage in M&A, these challenges can be even more daunting; however, identifying potential risks early can preserve corporate value, especially when complex legal and regulatory concerns are involved.

Emerging Areas of Transaction Risk for 2023

SOURCING & SUPPLIER LIABILITY

Third-party risk in the supply chain can be difficult to identify but can drastically alter the economics of a deal if uncovered post-transaction.

CYBERSECURITY VULNERABILITIES

Be diligent in reviewing an acquisition target's existing cybersecurity protocols and its track record of dealing with prior security incidents.

ACQUISITION FINANCING

Lenders will likely seek to strengthen their positions vis-à-vis potential recession; expect more lender-friendly terms in deals.

BENEFITS AND EXECUTIVE COMPENSATION

The success of some deals are highly reliant on getting key employees on board; buyers need to weigh carefully how to incentivize key performers.

REGULATORY COMPLIANCE

Regulatory enforcement is ramping up, and compliance programs are the first line of defense in preserving corporate value when companies face scrutiny.

POTENTIAL LITIGATION CLAIMS

In addition to current litigation, buyers need to assess carefully a target's potential future litigation, given the recent spike in third-party claims.

COMMERCIAL CONTRACTS

Buyers will need to examine carefully existing and new contracts for changes disadvantageous to the business in a recessionary environment.

ACCOUNTING PRACTICES

Economic downturns can tempt businesses to engage in questionable accounting practices; examine carefully a target's books for irregularities.

Private Equity Activity

Private equity deal values outpaced strategic M&A—reversing the trend of the previous year—as PE firms aggressively deployed capital and a faltering U.S. equities market provided more attractively priced targets. Notably, this dynamic ended abruptly late in the year as financing waned and stock indexes mounted a brief rally. There were no announced going-private transactions in November 2022, which, according to PitchBook, was "an almost unprecedented event in the last 17 years."

Given the experience of the past few years, it was no surprise to see that logistics, procurement, and supply-chain service providers were well represented among U.S.-based buyout targets, particularly during the latter half of 2022. Globally, packaging industry companies were the target of private equity interest, including a $3 billion investment in Italian packaging company Fedrigoni and the $1.3 billion buyout of Switzerland-based Bobst Group, a manufacturer of machinery for the packaging industry.

Large private equity buyouts in 2023 could be constrained by a lack of available debt financing, a characteristic of the changing interest rate environment. The issuance of debt related to leveraged buyouts in the U.S. declined by over 80 percent year over year during the second half of 2022. Rising interest rates have also contributed to unfavorable stock market valuations that have deterred private equity sponsors from exiting investments via public offerings. These factors could create opportunities for strategic buyers that can provide exit opportunities for private equity sponsors.

Notable Take-Private Transactions Since July 2022
Logistics, procurement, and supply-chain service providers were well represented among U.S.-based buyout targets, particularly during the latter half of 2022

ANNOUNCED DATE	TARGET	VALUE (MIL)	BUSINESS FOCUS
12/12/22	Coupa Software Inc.	$6,150.4	SaaS provider of business-spend management software, which helps companies manage the procurement process
9/28/22	BillTrust	$1,700.0	SaaS provider of products to manage billing, including consumer and business billing services
9/4/22	ChannelAdvisor	$725.0	SaaS provider of services that support marketing, fulfillment, and shipping
8/4/22	Atlas Air Worldwide	$2,909.3	Provider of aircraft leasing and outsourced air cargo and passenger operating services

Source: *PitchBook, "2023 US Private Equity Outlook"*

Distressed M&A

Year-end economic data for 2022 do not suggest that a robust bankruptcy cycle is immanent, especially in the U.S. manufacturing sector, which continues to post far lower bond default rates than the all-industry average. Nevertheless, some pandemic-related dislocations are only now creating financial distress for companies that have experienced extreme volatility in supply and demand over the past few years. Some manufacturers (makers of exercise equipment, gambling machines, and certain lines of consumer electronics come to mind) have been profoundly affected by this supply-and-demand whipsaw, and for those that entered this period highly leveraged, the result has been acute financial distress.

As global recession risks mount in 2023, there could be a greater opportunity for strategic buyers to target distressed companies and their assets. Bankruptcy and insolvency proceedings often allow for the sale of assets free and clear of liens and claims (including successor liability), a favorable position for buyers.

Manufacturers should be alert to opportunities to grow and/or refocus via corporate transactions, but buyers—particularly those that rarely undertake M&A—need to be aware of the challenges associated with integration and to use the diligence process to get a head start on realizing value post-transaction.

COMMERCIAL CONTRACTING

Business agreements in connection with the delivery of products and services have been buffeted by price volatility and supply constraints, straining longstanding relationships and making it difficult to strike upon adequate risk-sharing mechanisms.

The post-Covid supply chain debacles have stressed the delicate symbiosis between purchasers and vendors and have had a great impact on the way businesses approach commercial contracting. Terms that were boilerplate in nature not so long ago, like *force majeure* provisions, are now the subject of intense focus and negotiation. Furthermore, courts and counterparties have established this scrutiny as the new normal. What is perceived as "unforeseeable" in the context of contract disputes has shifted since the onset of the pandemic.

As the pivotal year of 2020 fades into history, businesses are approaching contracts with much more attention on risk. Given the elevated levels of inflation—which are expected to persist into 2023—and the continuing scarcity of key inputs, disputes will most certainly erupt from time to time, and the viability of certain complex risk-sharing contract provisions will be tested—both in and out of court.

There are some ways manufacturers can manage risk across the breadth of their commercial contracts, and chief among them is clarifying who is responsible for what in the contracting process and how that division of labor impacts key resources, such as the contracting team, IT, marketing, and the legal department. Manufacturers should carefully analyze their strategies to make sure the right people and resources are being deployed in the appropriate ways.

Who is Responsible for the Contracting Process?
Percent that believe their department plays the central role in contracting

Source: *EY, The 2021 EY Legal Survey, May 12, 2021*

This is an important consideration when viewed alongside the other key to contract risk management: distinguishing between complex, enterprise-altering contracts, and less complex, run-of-the-mill contracts. While the more routine contracts consume fewer resources on an individual basis, the sheer volume of routine contract work can divert resources from more important contracts. According to EY, routine contract work accounts for 40% of company contract resources.

Contract Lifecycle Management

Contract Lifecycle Management (CLM) is at the heart of an organization's ability to efficiently manage the volume and priority of their contracts. This includes intake or contract creation, negotiation, maintenance, renewal, and termination.

What is the meaning of the term CLM?

PROCESS OF GAINING CLARITY AND VISIBILITY AND MANAGING THE CONTRACTING LIFECYCLE	49%
A TECHNOLOGY SOLUTION THAT SUPPORTS AND ENABLES THE CONTRACTING LIFECYCLE	43%
IMPROVING DECISION-MAKING THROUGH ENHANCED CONTRACT DATA MANAGEMENT	4%
IDENTIFYING AND ALIGNING ROLES AND RESPONSIBILITIES FOR CONTRACTING	2%
OTHER	2%

Source: *WorldCC, CLM, Building the Case for Change Survey, September 2022*

At one end of the CLM spectrum, there may be manual tracking of contracts with filing on individual computers, or worse, in file cabinets. Renewal dates or triggering provisions might be tracked on spreadsheets or within electronic documents, if at all. More sophisticated approaches might comprise countless integrated systems that allow an organization not only to govern the flow and approval of all contracts through the business, but also track the metadata associated with those contracts.

Having a sophisticated CLM system—and the people to administrate such a system, whether in the legal, procurement, or business development departments— presents an opportunity for an organization to create a competitive advantage, or at a minimum, level the playing field with its competitors.

THE BENEFITS OF CONTRACT LIFECYCLE MANAGEMENT

At its October 2022 annual meeting in Las Vegas, the Association of Corporate Counsel (ACC) recognized Western Union and Husch Blackwell for a unique law firm-corporate legal department initiative that materially reduced costs and improved outcomes in the area of contract lifecycle management (CLM). In recognizing the collaboration as a **2022 Value Champion**, ACC noted that the team decreased outside legal spend by 18 percent. The savings in year two are forecasted at almost 70 percent. The program also has broken volume records on contracts reviewed by the company, all while reducing average contract execution time by 65 percent and improving collaboration between the legal department and procurement. Husch Blackwell developed a library of contract templates, playbooks, and processes customized for Western Union's unique needs and that serves as the "brain" of the program, allowing efficiencies that were previously unattainable.

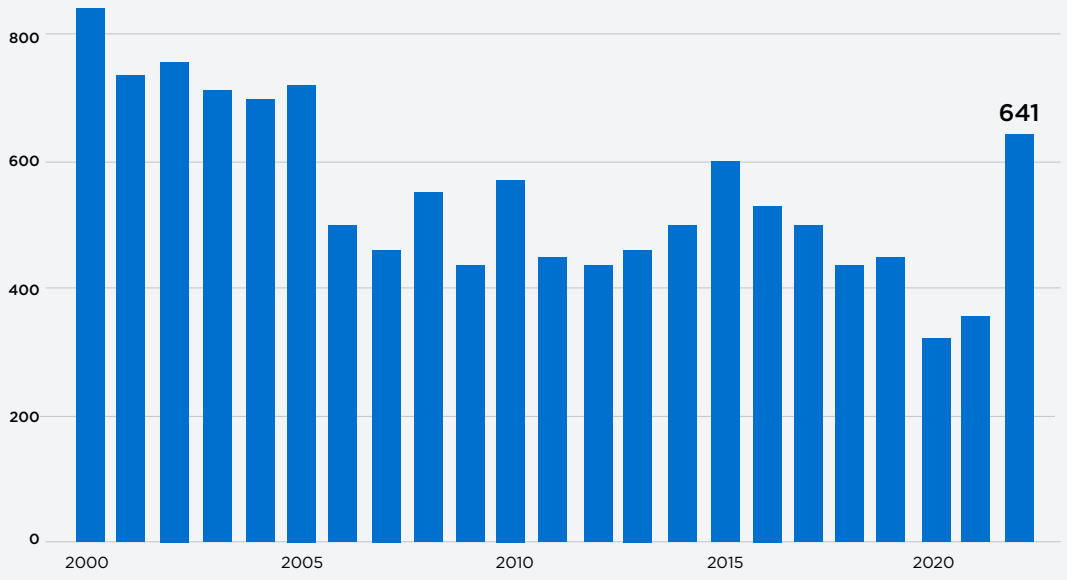
This marks the third time that ACC has recognized Husch Blackwell as a Value Champion. The previous client collaborations included Express Scripts Inc. (2017) and Monsanto (2018).

Manufacturers are intensely focused on hiring and retaining highly skilled employees whose skills are difficult to replace and much needed during a period of rapid change in the industry.

Unionization Trends in Manufacturing

The manufacturing, transportation, and warehousing industries saw a significant increase in union activity in 2021. According to data from the National Labor Relations Board (NLRB), 2022 has been no different. Thus far in 2022, unions have won more elections than any time since 2005—80% more than in 2021 and representing more than twice as many workers. In addition, petitions for future elections were up nearly 60% in the first nine months of the year, and we do not expect to see the move towards increased union activity subsiding anytime soon because of the overwhelming approval rate for unions. According to a recent Gallup survey, 71% of Americans approve unions, which is a high mark since 1965, up from 64% pre-pandemic.

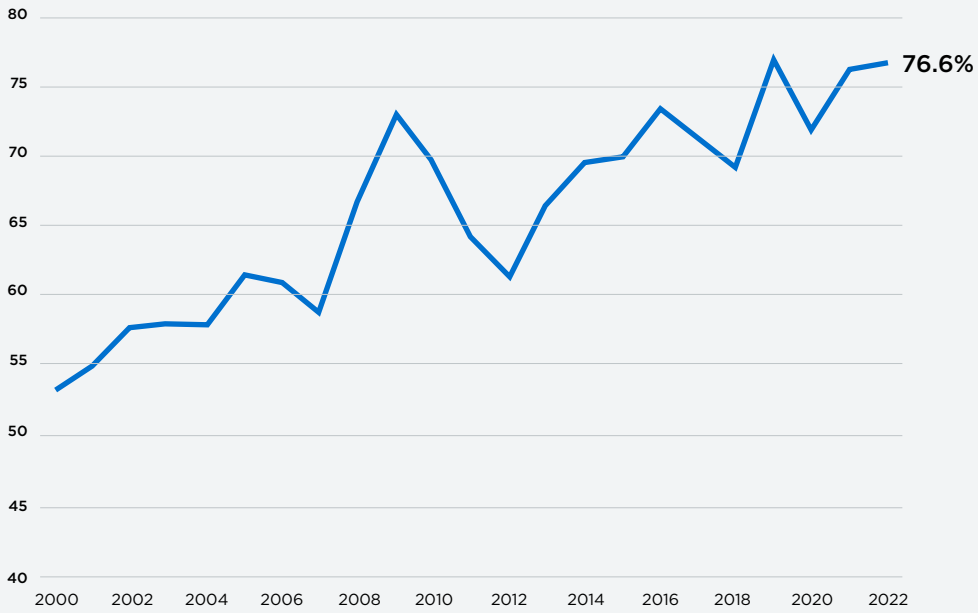
Organized Labor Unionization Elections, 2000-2020
Data for National Labor Relations Board elections, January through June each year.



Source: Bloomberg Law

According to data from the Cornell University Worker Institute Labor Action Tracker, the manufacturing, transportation, and warehousing industries have seen 134 labor actions since January 1, 2021, across 182 locations. In 2021, the manufacturing industry made up 17.7% of work stoppages, with an additional 10.6% contributed by the transportation and warehousing industries. Demands include a $15 minimum wage, Covid-19 protocols, first contract, health and safety, healthcare, job security, pay, and retirement and benefits, among other areas.

Organized Labor Winning Percentage in Unionization Elections
Data for National Labor Relations Board elections, January to June each year.



Source: Bloomberg Law

Given the rise in union activity, employers should be increasingly aware of employees' rights to engage in activity covered by the National Labor Relations Act (NLRA), including union organization efforts by employees and increased bargaining efforts by existing unions. Employers should especially be on the lookout for activity by non-union employees—also called "protected concerted activity"—that may still be covered under the NLRA. Companies should be aware that their employees have a right to join together to speak out publicly and to discuss among themselves things such as improving wages and working conditions, even though they are not unionized. Employers should note the NLRB has long held that an employee's protection continues even if that employee makes a false statement in the course of their protected concerted activity. This means that an employer generally cannot discipline or discharge their employee for doing so. Exceptions to this rule are possible; however, they are difficult to obtain.

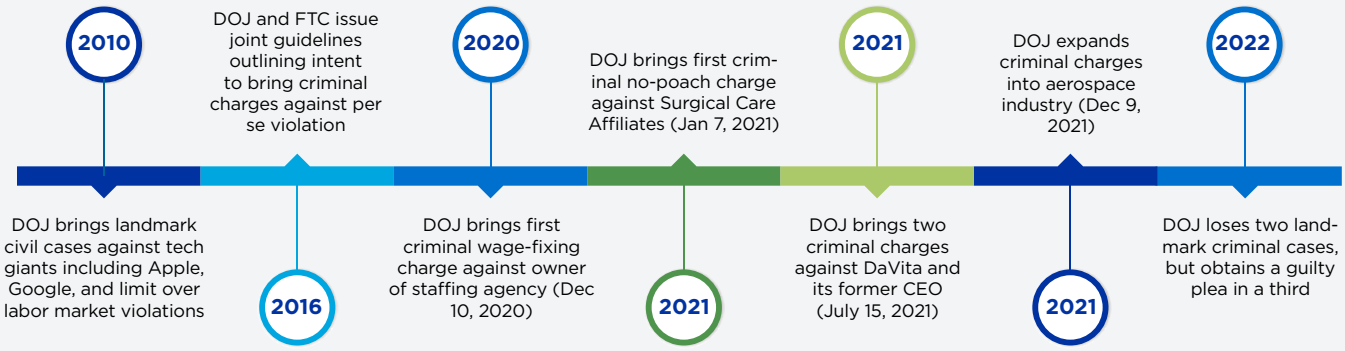
This movement towards increased union activity has reversed a decades-long reduction in unionization and could signal a new longer-term trend, although such trends are also dependent on the enabling political and policymaking environment. President Joseph Biden has publicly vowed to be the "most pro-union president ever." This coupled with massive media attention on union organization across the country has provided strong political wind for the sails of organized labor. With this said, it continues to be vital for employers to take special attention and proactive measures to avoid adverse action, or even the appearance of it, due to employees' protected concerted activity.

Noncompetes, Wage-Fixing and No-Poach Agreements

In industries that compete fiercely for talent—and manufacturing certainly falls in that category—decisionmakers may be tempted to seek out arrangements with competing entities to mutually limit or prevent the poaching of each other's employees; however, the United States Department of Justice Antitrust Division (DOJ) and the Federal Trade Commission (FTC), which both enforce federal antitrust laws, have recently turned their attention to "naked" no poach agreements (i.e., agreements not to solicit or hire another entity's employees that are separate from and not reasonably necessary to a larger legitimate collaboration). Specifically, the DOJ and FTC are taking the position that naked no-poach agreements are per se illegal and that companies and individuals that enter into such agreements may be subject to criminal prosecution.

In October 2016, the DOJ and FTC released "Antitrust Guidance for Human Resources Professionals," which was intended to alert human resources professionals and others involved in business decisions of actions that may violate antitrust laws. In the document, the DOJ and FTC reminded employers that businesses that compete to hire and retain employees are considered competitors in the employment marketplace, even if they do not offer the same products or services. Thus, they advised that naked no-poach agreements, whether written or unwritten, are illegal. Prior to the 2016 Guidance, the DOJ had brought civil enforcement actions against companies for entering into naked no-poaching agreements, such as agreements not to cold call each other's employees. Of note, the Guidance highlighted that the DOJ had previously brought three civil enforcement actions resulting in consent judgments against high profile technology companies for allegedly entering into no poaching agreements. The DOJ warned companies in the Guidance that it intended to criminally prosecute companies and individuals for entering into such agreements moving forward.

Key DOJ Labor & Employment Actions Since 2010



Source: *Adapted from Bloomberg Law*

In July 2021, the DOJ acted consistently with its warning in the 2016 Guidance. It announced that a federal grand jury returned an indictment charging DaVita Inc. and its former CEO with violating the Sherman Act by allegedly entering into agreements with other entities not to solicit each other's employees. On April 15, 2022, a jury found DaVita and its former CEO not guilty of violating the antitrust laws. This verdict came the day after a jury returned a verdict in the DOJ's first criminal wage-fixing case (a topic also addressed in the 2016 Guidance), finding the defendants not guilty of violating the Sherman Act.

Despite these setbacks for government prosecutors, DOJ did obtain its first guilty plea in October 2022 from a staffing company for allegedly entering into an agreement with another contract staffing company not to recruit or hire each other's nurses and to refuse to negotiate any further wage increases with their nurses. Throughout the course of 2022, the arc of regulatory action was clear. The DOJ is likely to continue prosecuting companies and individuals for entering into naked no-poach agreements. As such, it is critical that companies train their employees who are responsible for making hiring decisions and decisions regarding employees' terms and conditions of employment as to actions that may implicate antitrust laws. For example, human resources professionals must be cognizant that even a verbal or informal agreement with another company not to solicit each other's employees could be prosecuted by the DOJ. Moreover, to the extent an entity believes it has a legitimate basis for entering into a non-solicitation or no-poaching agreement with another entity, it is critical that counsel is involved in crafting the agreement in order to ensure the risk of running afoul of antitrust laws is minimized.

CYBERSECURITY

The scope and nature of cybersecurity threats are widening, even as efforts to combat crime have proliferated. Preventive measures are absolutely necessary; however, preparing for the worst-case scenario needs to be a staple of corporate culture.

The defining feature of corporate cybersecurity over the past decade has been the escalating nature of threat and response. As fast as technologists and security firms develop new approaches to thwart a species of threat, cybercriminals probe new weaknesses with new tools and tactics, leading to a vigorous arms race.

There were an average of 704 cyber attacks per week on companies in the manufacturing industry in 2021, according to Check Point Software, a network security company. By midyear 2022, that number had increased 33 percent. In response, corporations boosted information security budgets by an average of 26 percent throughout 2022. These investments have made a difference, reducing vunerabilities in the underlying technology, particularly in cloud security, which has seen an astounding 35-fold increase in global spending since 2017. Cybercriminals, however, are simply moving on to target other perceived weaknesses, and more often than not, those weaknesses are human, not technological. According to S&P Global, 82 percent of successful data breaches during 2022 were traceable to some form of human error. Manufacturers have spent substantial sums to harden their technology systems; the next battlefield against cybercrime will be corporate culture.

Information Security Spending Worldwide 2017-2023*, by Segment (in million U.S. dollars)

	2017	2018	2019	2020	2021	2022	2023	% INC.
APPLICATION SECURITY	2434	2742	3095	3333	4963	6018	7503	208.3%
CLOUD SECURITY	185	304	439	595	4323	5276	6688	3515.1%
DATA SECURITY	2563	3063	2662	2981	3193	3500	3997	56.0%
IDENTITY ACCESS MANAGEMENT	8823	9768	9837	12036	15865	18019	20746	135.1%
INFRASTRUCTURE PROTECTION	12583	14106	16520	20462	24109	27408	31810	152.8%
INTEGRATED RISK MANAGEMENT	3949	4347	4555	4859	5647	6221	7034	78.1%
NETWORK SECURITY EQUIPMENT	10911	12427	13387	15262	17558	19076	20936	91.9%
OTHER INFORMATION SECURITY SOFTWARE	1832	2079	2206	2306	1767	2032	2305	25.8%
SECURITY SERVICES	52315	58920	61979	65070	71081	71684	76468	46.2%
CONSUMER SECURITY SOFTWARE	5948	6395	6254	6507	8103	8659	9374	57.6%
TOTAL	101543	114151	120934	133411	156609	167893	186861	84.0%

*2022 and 2023 totals are projected.

Source: *Gartner*

In this regard there is a lot of work to do. Particularly in the aftermath of Covid and with the rise of remote work, businesses are challenged to inculcate cybersecurity best practices consistently throughout their workforces, and sometimes, the lack of training goes to the top of the organization. Take, for example, one notable data breach at a popular ride-hailing company that resulted in the 2022 criminal conviction of the company's security chief who chose not to report the incident—that was in addition to the company paying $148 million to settle private civil litigation. Being the victim of a cybercrime is bad enough, but the choices that leadership makes in the hours, days, and weeks that follow breach discovery can greatly compound an already difficult situation. It is best to approach things from a worst-case scenario and then plan accordingly, train rigorously, and test the protocols consistently. If you wait for the breach to occur, you will likely have a set of options that range from bad to worse.

Regulatory Responses to Cybersecurity

The escalating threat posed by cybercrime has led to a varied and robust regulatory response across multiple government agencies. Perhaps most notable was the unveiling in October 2021 by the Department of Justice of its Civil Cyber-Fraud Initiative (CCFI), an effort to "combat new and emerging cyber threats to the security of sensitive information and critical systems." CCFI attempts to expand the scope of the False Claims Act (FCA), a Civil War-era piece of legislation meant to address fraud in federal contracts, by applying the false certification theory of liability to certain contracts. In effect, the effort seeks to punish contractors that knowingly misrepresent their internal cyber controls and security or knowingly fail to timely report a cyber incident, presumably even if the failure to disclose did not result directly in harm to the government. CCFI has made cybersecurity a material component in the area of procurement, and manufacturers need to understand this evolving nexus between cybersecurity and government contracting.

Cybersecurity Trends to Watch in 2023

CHANGING THREAT LANDSCAPE
Defense is maturing, but as technology evolves — and weaknesses remain — attackers are thriving

SOVEREIGN THREATS
Cyberwar may now be an integrated part of nation-state conflict

INCREASING DISCLOSURE
Regulatory bodies and investors are expanding disclosure demands around cybersecurity and cyber incidents

THIRD-PARTY CYBERSECURITY RISKS
Increased reliance on third-party vendors increases systemic risks

CYBER INSURANCE
The role of insurance in risk mitigation is undergoing significant change

CYBERSECURITY AND RISK MANAGEMENT
Cybersecurity must become an embedded part of an entity's risk management

Source: *S&P Global, "Cyber Trends and Credit Risks," October 25, 2022*

The expansion of FCA into the cyber arena is part of a larger theme of federal cybersecurity regulation, where older laws—many of which predate the internet itself—are being retooled for new purposes. The Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Federal Trade Commission Act, Health Insurance Portability and Accountability Act, and the Defense Federal Acquisition Regulation are just a few of the laws that can be asserted in the cybersecurity setting.

For publicly traded companies, the Securities and Exchange Commission has proposed new rules in 2022 that would mandate reporting of "material" cybersecurity incidents within four days of discovery as well as periodic status updates of those incidents. The SEC also proposed disclosure requirements pertaining to "policies and procedures to identify and manage cybersecurity risks," management's role in implementing those policies, and the board of directors' cybersecurity expertise, if any. The new rules await completion, likely some time in early 2023.

Pillars of Data Breach Response

SECURITY

Abate ongoing attacks immediately and harden the system; remember, at the point of incident discovery, it is likely the intruder has been in your system for an extended period of time.

FORENSICS

Use outside independent forensics specialists to understand the contours of the incident; your IT team will likely not have the necessary skills, and using independent investigators will look better when the inevitable class action lawsuit comes.

REGULATORS

Know your regulators! For instance, for data privacy and PII-related issues, it's a state-by-state framework. All incident response plans need to contain a directory of agencies relevant to your business.

PUBLIC RELATIONS

If facts are unsettled or unknown, do not hazard guesses and estimates. Wait for the facts and then present one consistent message. Layered disclosures and walk-backs are deadly.

NOTIFICATIONS

Once decisions have been made regarding materiality, this process needs to operate flawlessly. Hire a vendor to manage it—it is complex, and there are no do-overs.

LEGAL

It is crucial to establish attorney-client privilege with the full response team, including the third-party forensic team. Privilege is not retroactive.

LAW ENFORCEMENT

Seek a law enforcement delay if PHI or PII involved in order to toll notification requirements. Some notifications are potentially exempt from this tactic, such as the SEC's proposed disclosure rules.

INSURANCE

Don't miss notification deadlines vis-à-vis cyber incidents and be sure to comply with all policy provisions regarding coverage.

STAKEHOLDERS

The more siloed the security function, the more important it is to have active communications with the c-suite. Stakeholders might also include less obvious parties, like vendors or customers.

PERSONNEL MANAGEMENT

Investigation of the incident could uncover negligence or incompetence within the ranks. Be prepared to shake up the team if necessary

2023 Legal Insights for Manufacturing Editorial Team

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

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

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

Jackson Otto
Partner | The Link
314.480.1835
jackson.otto@huschblackwell.com

Beau Jackson
Partner | Kansas City & Washington, DC
816.983.8202
beau.jackson@huschblackwell.com

Tyler Paetkau
Partner | The Link
510.768.0660
tyler.paetkau@huschblackwell.com

Jeff Jensen
Partner | St. Louis
314.345.6464
jeff.jensen@huschblackwell.com

Carlos Rodriguez
Partner | Washington, DC
202.378.2365
carlos.rodriguez@huschblackwell.com

Anne Mayette
Partner | Chicago
312.341.9844
anne.mayette@huschblackwell.com

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

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

Chris Sundberg
Partner | Denver
303.749.7235
chris.sundberg@huschblackwell.com

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