Published on *The National Law Review* https://natlawreview.com

Top Legal Issues Facing the Manufacturing Sector in 2023

Article By:

Vanessa L. Miller

Nicholas J. Ellis

Aaron K. Tantleff

John E. Turlais

Gregory Husisian

Agility and resiliency remain essential attributes for manufacturers in 2023. Manufacturers are no longer focused on figuring out when things will return to “normal.”

Instead, they are applying lessons learned from the past few years to evolve their operations to succeed in this “new normal.” Foley & Lardner’s Manufacturing Sector team continually examines these transformational shifts through the eyes of our clients and is well-positioned to help clients stay ahead of global trends and innovate in a dynamic marketplace.

As we embark on the second half of 2023, this second annual Manufacturing White Paper examines the business and legal considerations that continue to impact the industry and offers the perspectives and insights of attorneys with deep experience serving as trusted advisors to manufacturing companies.

Table of Contents

- 2023 CPSC and FDA Enforcement Trends
- Terminating Reseller Relationships Amidst the Network-Consolidation Trend: What Manufacturers Need to Know
- Top Environmental Issues Facing the Manufacturing Sector: The EPA Tackles Climate Change and Emerging Contaminants
- SEC Final Rules Mandating Compensation Clawbacks in Connection with a Restatement or Revision
- 2023 Manufacturing Sector M&A: Outlook and Tools to Maximize Strategic Transactions
- The Dawn of Generative AI in Manufacturing: Opportunities, Implications, and the Future

Everything Electrified and Connected All at Once: New Challenges Facing Supply Chains, Best Practices and Lessons Learned

Modern manufacturing and supply chains are in the midst of a sea change, as products continue a seemingly inexorable march toward electrification and greater connectedness. While these two trends are common across many industries, perhaps nowhere are they more pronounced than in the automotive industry. Most major automobile manufacturers have set aggressive goals to electrify their fleets, many in the range of 40-50% by the mid-2030s. At the same time, infotainment systems and other features have grown increasingly complex (and powerful) as many manufacturers are developing components and assemblies that contain integrated software and technology. Beyond the automotive industry, even the most basic household appliances are now wireless and connected. We have long since passed the point at which a basic automobile surpassed the computing power of a NASA space shuttle. It is (perhaps) only a slight exaggeration to suggest we may see a day in the not-too-distant future when our coffee makers do so as well.

The movement toward electrification and connectedness presents manufacturers with both opportunities and challenges. Those who take advantage of these opportunities and adapt to the changing landscape will thrive. Those who do not will see their market shares diminished and, ultimately many may not survive.

Opportunities: Innovation and Reinvention

Significant changes in manufacturing and supply chains present a new competitive landscape and opportunities for manufacturing companies. With these changes comes the need for new technologies. New technologies bring new players, including new companies. Some of these new companies are truly “new” in the literal meaning of the word. They are startups created to monetize new technologies and products. Other “new” companies that may present opportunities may have been around for some time, they can be considered “new” to a particular field or industry such as legacy automotive manufacturers as they expand their traditional internal combustion engine (ICE) offerings to include more electric vehicles and incorporate autonomous and other connected technologies. Both startups and legacy companies represent potential new business opportunities

and relationships for manufacturing companies.

New technologies and new customers present a growing demand for new products or components and require supplier capacity to manufacture those products or components for the market. There also is a need for new and innovative solutions to meet the demands of these changing technologies. These opportunities may be even more attractive because, in many of these new fields, there is less status quo or established market players, which can make breaking into the field less of a challenge for new participants. All of this adds up to significantly more opportunities for companies that are able to seize the initiative.

Challenges: The Risks Surrounding Novelty

While change brings many opportunities, it also brings challenges, including new technologies, new companies, and new relationships. No, that is not a mistake; these are indeed the same things that we listed in the previous section as opportunities. While “new” presents many opportunities, the flipside of those same opportunities are the elements of risk.

In the case of new technologies, there always will be some degree of working out the kinks, both with respect to performance and durability. The most obvious way in which these risks can manifest is through warranty claims and customer complaints. However, they can present other risks as well. For example, a supplier may make significant investments in production capacity for a customer bringing a new product to market. However, if the customer is unable to fully validate the product and launch is delayed or volumes reduced, the supplier can be left with unrecovered investments. The fact that many of these risks are unknown and lack historical data or precedent can make it more difficult for companies to price these risks into their cost walks when quoting new business.

Dealing with new companies in an industry (as either a supplier or a customer) brings its own set of challenges. New companies often have a limited track record or, in the case of legacy companies expanding into new fields, a limited track record within that particular field. They may also have a different worldview that can cause friction, or at least miscommunications and misaligned expectations between different companies. Perhaps the most commonly cited—although at times overstated—examples of such differing cultures coming together is the difference in cultures between traditional automotive manufacturers and companies in Silicon Valley. New companies may have limited resources and expertise necessary to overcome hurdles that may arise. Particularly in the case of startups or other new ventures, there may also be questions about whether new companies have the financial resources to meet their contractual obligations, should challenges arise.

All of these risks can be further compounded when they occur in a new relationship with a new customer or supplier. Unlike many well-established relationships (assuming they have been good relationships), newer relationships do not have the track record of trust and historical understanding on which to fall back when things get difficult. New business partners are more likely to question the motives, sincerity, or even ability of the other side, and can be more likely to reach for legal remedies should problems arise in the relationship.

Strategies and Best Practices

While the movement toward electrification and connectedness in the automotive and other industries can present challenges, there are a number of strategies and best practices that companies can employ to mitigate the risks these challenges pose.

1. **Consider your approach to software and integrated technology.** Whether your company will develop, license, or own a particular software or integrated technology will be a major strategic driver. The key question that many manufacturers will face is “to build or to buy?” Each path comes with its own list of pros and cons that need to be carefully considered in the context of the companies’ abilities, particular product, related costs and marketplace leverage.

2. **Strong contracts to protect against risks posed by new technology and new business partners.** In a changing world, one of the most important steps that companies can take to protect themselves largely remains the same – protecting themselves through their contracts. Companies entering into a new supply relationship should give careful consideration to the key terms of the arrangement, including at least the following: (i) quantity, (ii) term/termination, (iii) price (including price adjustment), (iv) warranties, (v) indemnification, (vi) intellectual property, (vii) choice of law/forum, and (viii) force majeure. For example, companies that are concerned about the performance of a new supplier’s technology should ensure that any purchase contract includes strong warranties and other assurances of performance. Companies that may be concerned about the viability or performance of a supplier should consider seeking licenses or other rights that would enable to obtain vital components from another source if the supplier does not meet its obligations. This directive is not limited to supply contracts alone. Any contract into which a company is entering to take advantage of the opportunities presented by these changes should be carefully considered and calibrated for the risks presented by that particular opportunity.

3. **Consider the form of the relationship to mitigate potential risks.** At the outset, companies can mitigate a significant amount of their potential risks and maximize opportunities by properly considering what form the relationship should take. For example, does it make sense to enter into a traditional customer supplier relationship? In some cases the answer may be yes; however, this is not always the case. For example, if a potential new supplier has developed a technology that your company wants to take advantage of but has no track record of production or manufacturing facilities, it may be more appropriate to consider an alternative structure such as a licensing agreement or some form of joint venture. Larger customers that want to ensure long-term access to technology may prefer to protect that investment through some form of investment, or even outright purchase of a provider rather than through a supply agreement alone.

4. **Due diligence, including promised technology and IP rights.** It should go without saying, but companies can avoid many headaches (or at least fully understand what they are getting into) by properly vetting their prospective business partners. Key issues to consider include looking at the technological, financial, and operational resources of a prospective business partner to ensure that they are able to perform their obligations, but also looking at their reputation and track record. For example, a litigation search can be very telling. If a company has been in business long enough, it is inevitable that a company will have some kind of litigation history. However, certain issues can present significant red flags. For example, if a company is facing litigation challenging its intellectual property rights or alleging infringement, this may present a significant risk as to whether the company has viable rights to the technology it is offering. Other examples require little or no explanation – if a company has been sued by multiple suppliers in the last month for nonpayment, it probably does not present a

good opportunity as a new customer. Finally, appropriate diligence should be performed on any new or unproven technology being offered, with a view to the "golden rule" – if it sounds too good to be true, it very well might be.

Adapting to a Changing Landscape

Unfortunately for some companies, creation and progress often involve a measure of destruction. Changing technology inevitably will leave some companies behind. In few places are these risks more evident than in the automotive industry as the shift to electrification in particular represents a fundamental change to the demands placed on the automotive supply chain. There undoubtably will be challenges along the way and it may take longer than the currently expected 10-15 years, but the path is largely locked in as most automotive manufacturers and their supply base are committing to investments in electrification. For companies that primarily manufacture products that are used only in traditional internal combustion engine vehicles – for example, fuel tanks – this presents a clear and obvious problem. How many companies can survive a 40-50% decline in their business?

Companies facing these changes need to consider carefully what their future looks like in the medium- to long-term horizon and develop a plan for how they will adapt. Key factors to consider include such considerations as:

- What does your company's product mix look like now, and how will those products be affected by impending changes in the industry?
- What new products are going to be needed as a result of these changes?
- How are software or new technologies integrated with your products (or how can they be integrated)?
- Who are your customers?
- Where do you need to be located geographically?
- How about your supply base and their geographic locations?
- What is the appropriate structure for a strategic partnership with a particular customer or supplier?

Once a company has assessed its risks and developed a plan to address those risks, it can move forward with making the necessary investments and changes to its business. If you haven't started, you are already behind!

Cybersecurity Threats in the Manufacturing Industry

In the hyper-connected era of Smart Manufacturing, accelerated by "Industry 4.0," manufacturing is undergoing a digital revolution. By leveraging technologies such as advanced automation, artificial intelligence, the Internet of Things, blockchain, and other technologies, manufacturers continue to

optimize production, increase efficiency, and drive innovation. However, this digital revolution brings complex cybersecurity risks and threats, creating significant implications for manufacturers.

For the second year in a row, manufacturing has been the most targeted sector by cyberattacks, accounting for nearly one in four incidents.[1] Throughout 2022 alone, ransomware attacks on the manufacturing industry nearly doubled, accounting for 72% of all ransomware attacks and implicating 104 unique manufacturing subsectors.[2]

As manufacturers increasingly integrate digital information technology with physical operational technology, the vulnerabilities that cybercriminals can exploit continue to multiply exponentially. Accordingly, while cybersecurity has always been an essential aspect of manufacturing, the increasing reliance on technology now makes cybersecurity one of the industry's most critical concerns. Below, we describe various types of cybersecurity risks and attacks faced by manufacturers and outline some of the legal implications and considerations that entities in the manufacturing industry should consider.

Types of Cybersecurity Risks Facing the Manufacturing Sector

Cybercriminals continue to target the manufacturing sector due to its integral role in the economy, potential critical industry and supply chain impacts, and vast amounts of sensitive data held by organizations within the sector. Cyberattacks may disrupt businesses and supply chains, undermining the benefits of digitalization and resulting in financial and productivity losses causing reputational damages.

These cybersecurity risks can be broadly categorized into malware attacks, social engineering attacks, and Advanced Persistent Threats (APTs), in addition to other risks unique to the manufacturing sector.

Malware Attacks involving the deployment of malicious software, may come in many forms, including viruses, worms, ransomware, and spyware, and constitute a significant threat to manufacturers as they can cripple an entire manufacturing operation, causing significant financial, operational, and reputational damage. This category of software is designed to infiltrate, damage, or disrupt systems. The most common malware affecting manufacturing is ransomware, which may involve the encryption and/or exfiltration of a victim's data and a ransom payment demand. Ransomware is especially dangerous for a manufacturer as it can halt production lines, disrupt operations, cause considerable financial loss, and significantly impact the global supply chain.

Social Engineering Attacks exploit human vulnerabilities rather than technological flaws to gain unauthorized access to systems and data, potentially leading to ransomware attacks or sensitive data theft. While phishing is a well-known form, social engineering attacks may involve spear-phishing (targeted at specific individuals or companies), baiting (enticing a user to perform an action with a false promise such as a free gift), and pretexting (creating a fabricated scenario to manipulate the victim into providing access or information).

Advanced Persistent Threats (APTs) are sophisticated, coordinated attacks that often target high-value industries like manufacturing. These attacks are typically conducted by highly skilled groups with substantial resources, intent on stealing sensitive information or disrupting critical infrastructure. In the manufacturing sector, APTs often target valuable intellectual property (IP), such as proprietary production techniques, research and development data, or business strategy documents. In addition to intellectual property theft, APTs can cause significant operational disruption as prolonged,

unauthorized access to a manufacturer's network may allow attackers to manipulate industrial control systems, disrupt production processes, or even sabotage equipment. APTs can also compromise supply chains. A successful attack on a manufacturer could give the attacker access to connected networks, such as suppliers, logistics partners, or customers. This potential for wide-ranging impact makes APTs a grave concern for the entire manufacturing ecosystem.

Intellectual Property Theft is one of the most coveted manufacturing targets for cybercriminals. Manufacturers often possess valuable proprietary information, including blueprints, manufacturing processes, research, and development data. Accordingly, sophisticated cybercriminal groups or state-sponsored entities may utilize APTs, among other cyber-attack tools, to target and exfiltrate IP. Given the value of proprietary information such as unique manufacturing methods, product designs, and research data, the impact of such theft on a manufacturing company can be immense, leading to potential market share loss, decreased competitive advantage, and substantial financial repercussions.

Supply Chain Attacks, often resulting from APTs, exploit the vulnerabilities in a company's supply chain network. Given the interconnected nature of the manufacturing industry, a single vulnerability can have far-reaching implications. Attackers can exploit weaker links, such as small suppliers with less robust security, to infiltrate larger, more secure networks. Notably, the 2020 SolarWinds hack, which affected government and corporate networks, was a supply chain attack.

Industrial Control System (ICS) Attacks, also often stemming from APTs, target industrial control systems crucial for modern manufacturing processes and can potentially give the attacker control over production processes. Such an attack can halt production, cause physical damage, or even result in safety incidents. Stuxnet, a malicious computer worm discovered in 2010, targeted ICS in Iran's nuclear facilities, highlighting the potential real-world implications of such attacks.

Insider Threats from disgruntled employees, contractors, or other insiders with access to critical systems can prove just as dangerous cybersecurity risks as threats from outside the organization. As with other types of cyber threats, insider threats pose a significant risk of IP theft. Notably, not all insider threats are intentional. While insiders might misuse their access intentionally, their credentials can also be co-opted through phishing or other methods, allowing an external attacker to infiltrate systems.

Third-Party Vulnerabilities involve cybersecurity risks that result from a manufacturer's relationships with vendors, suppliers, service providers, or any third parties that have access to their systems or data. In other words, a manufacturer's cybersecurity resilience is often only as strong as the weakest link in its supply chain. A third party lacking robust cybersecurity measures can become an initial vector for cybersecurity attacks.

Potential Impact on Critical Infrastructure

The manufacturing sector often serves as a backbone to critical infrastructure – the systems, facilities, and essential services that underpin the functioning of our societies and economies. This encompasses sectors such as power generation, water supply, transportation, telecommunications, and healthcare. Manufacturers play an instrumental role in supporting these infrastructures by providing essential components, equipment, and services necessary for their operation. Consequently, a cyberattack that significantly disrupts manufacturing processes can have wide-reaching and potentially catastrophic impacts on critical infrastructure, the economy, and national security.

Energy. A cyberattack on manufacturers in the energy sector, including those that provide parts for power plants, oil refineries, and wind turbines, could result in widespread power outages, leaving homes, businesses, and public services without electricity. This could affect thousands, if not millions, of individuals and cause significant economic damage. At an extreme, it could even have national security implications, as energy grids could be left vulnerable to additional attacks.

Transportation. Similarly, in the transportation sector, a successful cyberattack on manufacturers of automobile, aircraft, and train components could disrupt the availability of these parts and impact production. The cascading effect of such disruptions could lead to decreased transportation capabilities, major disruptions to the supply chain, and the availability of vehicles or goods, significantly impacting the mobility of goods and people and potentially even impacting military readiness if defense-related transportation is affected.

Telecommunications. In telecommunications, manufacturers produce everything from networking equipment to mobile devices. A disruption in manufacturing these products could have a ripple effect, causing communication blackouts that affect businesses, government agencies, and individuals. Such an event could severely disrupt daily operations across multiple sectors and hinder emergency response efforts.

Healthcare and Pharmaceuticals. When it comes to healthcare and pharmaceuticals, cyberattacks can have particularly dire consequences. For example, an attack on medical device or pharmaceutical manufacturers could result in medication production shutdowns, compromised medical device functionality, or altering the formulation of life-saving drugs. In the worst-case scenario, this could have severe repercussions on patient safety and public health.

National Security. Cybersecurity attacks on any of the critical infrastructure sectors noted above may have major national security implications, particularly if the targeted manufacturing company is involved in producing defense equipment or technology. A cyberattack on manufacturers supplying the defense sector could interrupt the production of essential military equipment, impairing a nation's defense capabilities, or result in our nation's enemies gaining access to the IP underlying critical defense technology. Similarly, disruptions in the energy or telecommunications sectors could compromise key national capabilities and intelligence operations.

Overall, the potential impact of cyberattacks on critical infrastructure underscores the urgent need for robust cybersecurity measures within the manufacturing sector. The interconnectedness of today's world means that a cyberattack on a single manufacturing company can ripple outwards to affect a broad array of unrelated sectors. Moreover, these attacks can undermine the public's trust in critical services, causing societal instability. Given the

potential scale of disruption and associated economic, health, safety, and national security risks, manufacturers must adopt a proactive approach to cybersecurity. Cybersecurity in the manufacturing sector is not merely an issue of business continuity, it is a matter of national and international security.

Legal Implications and Potential Liabilities

The legal implications of these cybersecurity attacks are vast, including significant financial and legal liabilities from various sources. First, manufacturers may face liability based on data protection laws if a cybersecurity attack involves a personal data breach. For example, if a manufacturing company controls large amounts of personal data, including customer or employee data, it would be subject to

data protection laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Privacy Right Act (CPRA) in the United States. A data breach that exposes or results from noncompliance with data protection laws could result in significant regulatory fines and penalties. For instance, the GDPR imposes significant financial penalties for noncompliance, up to 4% of annual global turnover or €20 million, whichever is higher. Additionally, manufacturers may face considerable liability arising from class actions filed by affected individuals.

Second, directors and officers of manufacturing companies could face legal action from shareholders based on an alleged breach of fiduciary duties. Such duties include the duty of care, which could be interpreted as an obligation to implement reasonable cybersecurity measures in the context of cybersecurity. If a cybersecurity attack results in significant financial loss and the shareholders can show that directors and officers failed to implement adequate cybersecurity measures, they could be held liable for breaching the duty of care. Similarly, if a cybersecurity attack results from a failure to properly vet and monitor a supplier or other third party's cybersecurity policies and procedures, manufacturers may face potential claims alleging a breach of the required duty of care. Shareholders may also file lawsuits alleging that negligence of the directors and officers resulted in financial loss.

Third, if a cybersecurity attack involves the loss or disclosure of IP, especially in the case of industrial espionage, a company may be found to be in violation of trade secret laws or be subject to IP lawsuits if the cybersecurity attack results in the theft and subsequent disclosure and/or unauthorized use of proprietary information.

Finally, under contract law, manufacturers could be held liable for breach of contract if a cybersecurity attack disrupts their ability to fulfill contractual obligations. Additionally, contracts often contain clauses related to required data protection and cybersecurity. This could lead to various legal consequences, including termination of contracts and liability for any resulting damages.

Recommendations for Manufacturers to Manage Cybersecurity Risks

Given the multitude of cybersecurity risks and significant legal implications, manufacturers must adopt and comply with robust cybersecurity measures and policies, including technical and legal measures.

Technical Measures. These include implementing multi-factor authentication, utilizing modern endpoint detection solutions, ensuring comprehensive business continuity and backup procedures, regularly updating and patching systems, conducting regular security audits, and training employees on cybersecurity best practices. Technical measures are the first line of defense against cybersecurity risks. Manufacturers should review their cybersecurity policies and procedures, and ensure proper technical security measures are implemented and followed.

Employee Training and Awareness*.* Employees often represent the most significant, and most difficult to manage, vulnerability in an organization's cybersecurity defenses. As such, regular employee training and awareness campaigns are crucial. Training should educate employees about the nature of cyber threats, the importance of cybersecurity measures, and their role in defending against them. Topics can include the importance of strong, unique passwords, the risks of phishing attacks, and the correct procedures for handling, storing, and sharing sensitive data.

Legal Measures. Manufacturers can also protect themselves by incorporating appropriate and compliant cybersecurity clauses into their contracts. For example, to mitigate the risks associated with third-party vulnerabilities, these clauses should specify third parties' responsibilities regarding

cybersecurity, including data protection obligations, required security measures, and the procedure for responding to cybersecurity incidents. Manufacturers should also ensure they conduct thorough cybersecurity audits of their third parties. These audits should assess the third parties' cybersecurity policies, procedures, infrastructure, and compliance with relevant regulations. These clauses and audits protect manufacturers legally and incentivize third parties to uphold high cybersecurity standards and limit liability in the event of a cybersecurity attack.

Cyber Insurance. Manufacturers also should invest in cyber insurance to mitigate financial risks associated with cybersecurity attacks, including the costs to investigate, remediate, and respond to such attacks, negotiations and ransom payments, and potential litigation that may arise. Additionally, manufacturers should strive to comply with applicable cybersecurity standards such as ISO 27001 and the NIST Cybersecurity Framework, as these standards provide guidelines and best practices for managing cybersecurity risks. Achieving and maintaining these certifications can demonstrate that the company has taken reasonable steps to protect against cybersecurity threats.

Consider Collaborating with Legal Counsel

Manufacturers face not only a multitude of cybersecurity risks but must also navigate the complex patchwork of cybersecurity and data privacy laws at the state, federal, international, and industry-specific levels. These often complicated laws can vary widely depending on the jurisdiction, industry, and the type of data a company handles. Legal counsel can identify the applicability and ensure compliance with laws like the GDPR, CPRA, and other comprehensive data privacy laws, including cybersecurity requirements imposed by the federal government under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), the Defense Federal Acquisition Regulation Supplement (DFARS), and Federal Energy Regulatory Commission (FERC), and other industry-specific regulations.

Legal counsel also can help identify potential liabilities and legal risks related to cybersecurity. This may include facilitating risk assessments, developing risk management strategies, including policies and procedures to mitigate cybersecurity risks, and preparing and executing an appropriate incident response plan following a cybersecurity incident to ensure compliance with applicable data breach privacy laws. Legal counsel can also assist in reviewing and revising contracts with suppliers, service providers, and customers to ensure the inclusion of appropriate cybersecurity requirements and protections, such as indemnification clauses or limitations of liability in the event of a cybersecurity incident. Finally, legal counsel involved and well-versed in a manufacturer's cybersecurity practices and procedures can more effectively assist in the event of litigation, whether from affected individuals, business partners, or regulators.

Managing cybersecurity risks requires a comprehensive, multi-faceted approach combining robust technical measures, strong legal protections, and a commitment to employee training and awareness. By implementing these measures, manufacturers can significantly reduce their cybersecurity risks and protect themselves from potential legal liabilities.

Conclusion

While offering significant advantages, the digital revolution in the manufacturing industry has exposed the sector to elevated cybersecurity risks. As cyber threats grow more sophisticated, manufacturers must navigate a complex legal landscape, balancing technologically supported growth with compliance with data protection laws, potential liability for cyber breaches, and the need for robust cyber defenses.

In this rapidly evolving context, proactive risk management and adherence to cybersecurity standards are not merely best practices but strategic imperatives. Manufacturers should continually revisit their cybersecurity strategies, aligning them with the latest technological advancements and regulatory updates. Fostering a strong cybersecurity culture will not only mitigate legal liabilities but will also contribute to the long-term resilience and competitiveness of the manufacturing sector.

[1] *See "X-Force Threat Intelligence Index 2023," IBM Security, February 2023.*

[2] *See "ICS/OT Cybersecurity Year In Review 2022," Dragos.*

The New Era of U.S. Customs Enforcement (and Compliance)

In recent years, the United States has experienced a notable shift in trade policies, marked by an increase in high-rate special tariffs and intensified enforcement measures implemented by U.S. Customs and Border Protection (CBP). These developments have significantly impacted the international trade for manufacturers. With the U.S. government using as a tool to protect domestic industries, promote fair trade practices, and address perceived imbalances with China, manufacturers who serve as importers of record need to prioritize customs compliance, both to mitigate risks and to maintain competitive positions in the evolving trade environment.

Customs Compliance Is Essential in the Current Enforcement Environment

Recent developments that have made customs a critical compliance area include:

- Unprecedented implementation of high special tariffs, including 10 and 25 percent Section 232 duties on aluminum and steel, Section 301 tariffs of up to 25 percent on nearly all goods from China, and a record number of antidumping and countervailing duty cases, which can impose tariffs into the triple digits.
- CBP's renewed emphasis on enforcement and revenue collection, given the much greater tariffs that it is now collecting.
- The long-awaited completion and full implementation of the Automated Commercial Environment (ACE) portal, which gives CBP the tools to run sophisticated searches to find anomalies in import patterns, including misclassifications, undervaluation of entered value, and erroneous country-of-origin declarations that can lead to large underpayments of customs duties.
- The New Enforcement priorities and increased budgets particularly with respect to forced labor issues, such as the requirements imposed under the Uyghur Forced Labor Act
- Increased use of electronic portals, such as the e-Allegations Program and the Enforce and Protect Act (EAPA) Program, by which members of the trade community can report suspected trade violations to CBP.

These developments signal a new paradigm of increased CBP enforcement. Notably, the change in presidential administrations did not result in any material changes to the U.S. international trade

policy. There continues to be bipartisan support to keep pressure on China (via high tariffs and AD/CVD orders) to deal with perceived Chinese government manipulation of the international trade, investment, and intellectual property norms. Other important developments, such as the migration to the ACE portal and the ability to report potential violations more easily online, are permanent fixtures.

Manufacturers that act as importers of record accordingly must remain vigilant in customs matters, including by implementing rigorous and consistent customs compliance procedures, such as those outlined below.

Customs Compliance Best Practices

Our recommendations for customs compliance are based on the expectations of CBP and long-standing work with importers. Some key items we recommend include the following:

- ***Start by Recognizing Your Company Is Ultimately Responsible.*** CBP regulations place the burden for accuracy in the importation and payment of duties on the importer of record – not the broker or freight forwarder, as some importers mistakenly believe. The importer of record is responsible for, among other things, accurately determining the country of origin, correctly classifying the goods, determining if any extraordinary duties are due, complying with all free-trade agreement requirements, ensuring goods are not a product of forced labor, and fully paying all tariffs. In the case of errors, standard broker agreements generally limit recovery to the nominal fees associated with each entry, while the importer of record remains fully responsible for all underpayments and associated penalties.

- ***Prepare a Customs Compliance Manual.*** Based on our experience in recent audits, CBP expects importers to go beyond a simple compliance policy and instead implement a comprehensive customs compliance program with a manual that includes written procedures and internal controls for each of the relevant elements of reasonable care. Importers that memorialize such measures in a customs manual tailored to its operations are less likely to have import-related errors and are in a better position to explain the scope and implementation of customs compliance programs to CBP auditors.

- ***Create a Customs Classification Index*****.** We recommend importers regularly review the products they import and confirm the accuracy of the associated HTS tariff classification codes. The U.S. government updates these codes periodically throughout the year, and new products may need new classifications. Importers should maintain the most current HTS classifications in a database that is available to their third-party customs brokers or other parties responsible for preparing customs entry filings.

- ***Review Product Valuations & Declared Value.*** Importers should review the methodologies used to calculate the ad valorem value of the products they import, paying particular attention to transactions involving related or affiliated companies. Notably, transfer pricing requirements under CBP regulations differ appreciably from transfer pricing requirements imposed by the IRS, thus often requiring manufacturers to prepare a customs-specific transfer pricing analysis Special attention is also necessary to determine whether the valuation includes all relevant off-invoice items, such as royalties and assists.

- ***Coordinate with Customs Brokers & Freight Forwarders***. Importers should engage with their freight forwarders and customs brokers to determine whether they are consistently following CBP requirements and should coordinate regarding required customs recordkeeping. These areas should not be left to customs brokers on their own because, as noted above, CBP will ultimately hold the importer of record responsible for any compliance lapses.

- ***Conduct an Internal Customs Compliance Audit.*** Importers who are at a heightened risk for a customs inquiry or scrutiny, such as companies that frequently import goods from China or goods subject to potential antidumping or countervailing duties, should consider performing an internal customs audit to determine whether existing compliance systems are effective. A good starting point for such an audit may be found in the questionnaire at the end of CBP's Importer Self-Assessment Pilot Program publication.

- ***Conduct Compliance Training.*** Importers should train relevant employees on CBP requirements annually. Such employees typically include customs compliance staff, procurement personnel, and individuals working in the company's shipping/ logistics departments. Relevant compliance topics include:

    - Importer of record responsibilities;
    - Classifying imported goods;
    - Determining countries of origin;
    - Making preferential tariff claims under the USMC and other FTAs;
    - Coordinating with customs brokers and freight forwarders;
    - Conducting post-entry checks and making corrections;
    - Tracking assists and other valuation issues; - related party pricing considerations;
    - Identifying and claiming relevant section 301 exclusions; and
    - Recordkeeping responsibilities.

- ***Evaluate USMCA/FTA Claims.*** Importers should review their use of FTA or other tariff duty preference programs to determine whether they are applying the eligibility criteria properly and have the documentation necessary to support their claims. If the goods come from Canada or Mexico, then claims for preferential tariff treatments should be evaluated against the USMCA rules, which often differ from the older NAFTA requirements. Some of the key issues to consider include:

    - Whether the imported goods meet USMC's regional content requirements;
    - Whether required certificates of origin are available at the time of entry (with appropriate blanket periods identified); and

    - Whether the company maintains all of the required documentation to support free-trade preferences for the appropriate period of time.

- ***Review Products for Antidumping and Countervailing Duties.*** Finally, companies should periodically review their imported goods to determine whether they may be subject to additional tariffs under various antidumping or countervailing duty orders.

Dealing with CBP Requests for Information: Informed Compliance Letters and Form 28s/29s

A relatively recent development is the issuance of "informed compliance" letters by CBP, a tactic we expect CBP will continue to use more in the future. These letters often are issued to major U.S. importers to encourage them to review their recent entries and determine if they have treated entries correctly where they acted as the importer of record. These letters often are sent to major importers who have not been audited in the past decade or that are viewed as being at a higher risk for violations. At the same time, CBP is sending out an increasing number of Forms 28s (requests for information) and Form 29s (notices of action), which CBP expects importers will broadly apply to all similar imports.

The receipt of these types of communications means CBP has reviewed the data of an importer of record and likely identified specific problems with its import transactions, putting the company at an increased risk of a comprehensive audit. According to CBP officials for informed compliance letters, the expectation is that companies that receive these letters will soon be the subject of a "focused assessment" or other type of CBP audit in the near future. The letters thus are a way of encouraging major importers to enhance their compliance and file voluntary self-disclosures in anticipation of the audit. To provide further "encouragement," CBP has indicated that companies that do not follow up with a voluntary self-disclosure can expect any subsequently discovered violations will be subject to higher-than-normal penalties. The letters warn not only of potential monetary penalties, but also the prospect of seizure or forfeiture of imported merchandise.

Best practices when receiving these types of communications from Customs include:

- Determining the scope of impacted entries;
- Preparing for a potential CBP audit;
- Reviewing customs compliance policies;
- Reviewing the care taken by its customs brokers;
- Conducting a risk assessment, including regarding the issues identified in the letter or Form 28s/29s;
- Determining if HTS classifications are correct and supported by the product attributes;
- Determining whether any post-entry adjustments are needed;
- Determining whether free trade preferences are supported by FTA certificates of origin

and appropriate regional content;

- Evaluating whether off-invoice items such as royalties and assists are appropriately recognized; and

- Considering whether there are any other issues in the company's import data to indicate compliance failures and penalty risks.

While the assessment should start with the issues identified in the letter, the review should be comprehensive. Further, the review also should cover the rigor of the importer's compliance measures and training, as these are evaluated by CBP in an audit. Any errors should be documented, and a plan put in place to strengthen the company's compliance procedures and internal controls to prevent their recurrence.

Voluntary Disclosure

If potential violations are discovered, the importer also should strongly consider filing a voluntary disclosure. This can be accomplished using an initial marker letter, which informs CBP that an investigation of potential compliance lapses is ongoing. The marker letter then is followed by a complete disclosure, (60 days by regulation), although it is possible to request a longer time period or later to request extensions.

Voluntary disclosure of violations to CBP – if done before CBP initiates a formal investigation of potential violations – can provide numerous significant benefits to importers of record. Most notably, voluntary disclosure often results in back payment of duties and interest owed, but no penalties, if the mistakes were the result of negligence. And, even in cases of gross negligence or fraud, voluntary disclosure can result in significant mitigation of penalties and enforcement actions if the disclosure is made in good faith and includes all relevant information.

Voluntary disclosure allows importers to take control of the investigation process. By promptly identifying and reporting violations, importers can proactively address the violations, implement corrective measures, and prevent similar violations from occurring in the future. This proactive stance can help importers avoid full CBP audits, as well as protect their reputation, maintain business continuity, and avoid potential disruptions to their supply chains.

Finally, voluntary disclosure can serve as a valuable tool for understanding CBP regulations and memorializing/ improving compliance best practices. This knowledge, in turn, will help mitigate future violations and – as we have found in a number of voluntary disclosures in which we have been involved – could lead the importer to discover tariff-saving opportunities that were missed in prior years.

Navigating the Domestic Content Compliance Minefield

"Buy American" requirements in U.S. federal contracts date back nearly 100 years, to the Great Depression, but the policy of trying to ensure federal dollars are spent on U.S.-manufactured products has never been more pervasive than it is today. Recent legislation authorizing new federal spending or creating new multibillion-dollar programs has made compliance with stricter domestic content requirements a precondition to the receipt of federal funds. It is safe to say that "Buy

American” or “Buy America” requirements—and, as will be discussed below, there is a difference—are having their proverbial moment.

While some federal agencies have historically applied certain “Buy America” requirements to their infrastructure programs, a portion of the 2021 Infrastructure Investment and Jobs Act for the first time required all federal agencies to impose domestic content requirements on infrastructure programs receiving federal financial assistance. The so-called “Build America, Buy America” Act—referred to as “BABA” for short—created a new set of domestic manufacturing and content requirements for manufactured products, iron and steel products, and construction materials that are continuing to be implemented through agency-specific guidance and waivers.

Manufacturers face several challenges in complying with these domestic content requirements, not the least of which is understanding what set of requirements applies to a particular product or a specific project. There is a common misconception that there is a single set of “Buy American” requirements, but the truth is that domestic content requirements can vary depending on the project, the product, or even how a product will be used on a specific project. Many projects require manufacturers to submit certifications of their products’ compliance with the applicable domestic content

Despite these challenges, these domestic content requirements also present an opportunity for manufacturers who understand the rules and have taken the steps necessary to ensure their sourcing and manufacturing processes pass muster under them. This article discusses some key strategies for assessing compliance with domestic content requirements.

Know What Domestic Content Rules Apply to the Project

It may seem self-evident to state that you need to know what the rules are to be able to ensure you comply with them, but that principle is especially salient in the realm of domestic content requirements. There are different regimes that apply to direct federal procurements of construction materials or supplies—such as a purchase by the U.S. Department of Defense—and to projects overseen by state or local government entities that have received federal financial assistance. Direct federal procurements are subject to the Buy American Act (“Buy American”), while projects receiving federal financial assistance are subject to a “Buy America” requirement, such as BABA. While there are some similarities between the two regimes, there are some important differences between “Buy American” and “Buy America” requirements.

Buy American. One significant difference is that Buy American Act contract clauses provide more flexibility for suppliers of commercially available off-the-shelf, or “COTS,” items. A COTS item is a product that is sold in substantial quantities in the commercial marketplace and is offered to the government without modification from the manner in which it is sold commercially. Under the Buy American Act, a COTS item is considered domestic so long as it is manufactured in the United States, without regard to the country of origin of the components of that COTS item. In other words, there is no cost-of-components test required for a COTS item under the Buy American Act.

If the value of the contract exceeds certain dollar thresholds—generally, $183,000 for purchases of supplies, and $7,032,000 for construction projects[1]— the Buy American Act requirements can be waived for products of countries with which the U.S. government has entered trade agreements. When this so-called “Trade Agreements Act” provision applies, the product of a trade agreement country is treated the same as a domestic product and can be supplied on the project without a waiver. This can provide the opportunity to supply products that are not manufactured in the United

States, provided they are manufactured in a country identified in the relevant contract clause as one subject to a bilateral or multilateral trade agreement to which the United States is a party.

Buy America. The "Buy America" requirements imposed by BABA are, in certain key respects, more onerous than those imposed under the Buy American Act for direct federal procurements. For example, a manufactured product—even a COTS item—is not considered "domestic" under BABA unless it meets two tests: (1) it is manufactured in the United States, and (2) its domestic-origin components account for more than 55% of the cost of all its components (the so-called "cost-of-components" test). The application of the cost-of-components test can be particularly tricky for manufacturers who are not familiar with the test and have not had occasion to assess the countries of origin of their products' components.

It is also far less likely that a manufacturer can use a product of a trade agreement country on a BABA project, because that would require the state or local government entity that is administering the project to be covered by the trade agreement. While there may be some state government entities that are covered by the World Trade Organization's Government Procurement Agreement, in practice very few state or local agencies receiving federal financial assistance on an infrastructure project will be subject to a trade agreement.

BABA Agency-Specific Implementation. Even under the umbrella of BABA, there can be variations in how the general requirements are implemented on specific projects. That is because each agency is responsible for implementing the BABA requirements, or a similar Buy America requirement, in the projects that it administers and funds. While there is overarching guidance provided by a central U.S. government entity—the Office of Management and Budget (OMB)—agencies can and have adopted their own waivers of the BABA requirements and, in some cases, have defined terms that remain undefined in the OMB guidance. Moreover, U.S. Department of Transportation (USDOT) agencies that had their own longstanding "Buy America" rules prior to BABA have generally continued to apply their existing "Buy America" requirements, sometimes with slight modifications to address new wrinkles added by BABA, such as the coverage of non-ferrous "construction materials."

Thus, knowing what federal agency is involved in overseeing a project subject to a BABA or "Buy America" requirement is critical to understanding the specific parameters of that requirement and what, if any, exceptions or waivers may apply.

Know What Domestic Content Rules Apply to Your Product

Once you have identified the relevant set of Buy American or Buy America rules governing a specific project, another critical aspect of compliance is figuring out how the product you manufacture fits into those requirements. One critical element is determining whether your product would be considered a "manufactured product" or would be subject to the special iron/steel sourcing rules for a predominantly iron or steel product. In the BABA context, non-ferrous construction materials are subject to their own set of sourcing and domestic manufacturing requirements. Knowing whether your product—or the product into which your product will be installed—will be treated as a manufactured product, iron or steel product, or non-ferrous construction material establishes the domestic manufacturing/sourcing standard to which your product will be held.

This exercise also requires an understanding of how your product fits into the supply chain for the project subject to a Buy American or Buy America requirement. Will your product be delivered directly to the customer or construction site? If so, your product would be directly subject to the applicable requirement.

But what if your product is being supplied to a higher-tier manufacturer who will integrate into that manufacturer's own product? Under that circumstance, your product would be at most a "component," if not a "subcomponent," of the product actually delivered to the customer or construction site.

The compliance considerations are usually different for suppliers of components or subcomponents. As one example, under BABA, there is no "cost-of-subcomponents" test for components. That means a component of a manufactured product is considered "domestic" under BABA so long as it is manufactured in the United States, regardless of the country of origin of its component parts.[2] In that case, your compliance obligation as a component supplier is to report the country of origin of your product to your customer, which will then have to assess whether it can meet the 55% cost-of-components threshold at the "manufactured product" level. Because components do not need to meet a "cost-of-subcomponents" standard, a component supplier would not need to address the domestic/foreign content of its product, only the country in which it is manufactured.

What Does U.S. "Manufacturing" Require?

The Buy American and Buy America regimes both require U.S. manufacturing, but the definition of "manufacturing" is hard to pin down. The term is not defined in the Buy American Act contract clauses themselves, nor is it defined in the statutory text of BABA. It is generally understood to require some type of processing that can be said to convert component parts into the end product sought by the government, but where and how to draw the line can become quite complicated.

The lack of a single definition of "manufacturing" is attributable in part to the variety of types of manufacturing processes. Different sources have articulated different definitions. For example, courts and the U.S. Government Accountability Office have framed domestic manufacturing as completion of the article in the form required by the government or making the article suitable for its intended use and establishing its identity as the relevant end product. Federal procurement regulations define the "place of manufacture" of an item as the place "where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government." These definitions are hardly black-and-white.

As a result, when a product has undergone significant processing outside the United States prior to arrival in the U.S. for final processing, the assessment of whether the U.S.-based processing is sufficient to constitute domestic "manufacturing" typically requires a fact-intensive analysis that evaluates the comparative time, complexity, and value of the processing operations performed in the U.S. and in foreign countries.

Establishing Processes to Ensure Buy America Compliance

The complexity and uniqueness of Buy America requirements places a premium on establishing processes to assess—and document—your ability to comply with those requirements. If you have both U.S.-based and non-domestic manufacturing sites for a particular product line, you need a process to ensure that only U.S.-manufactured products are supplied on a project subject to a Buy America requirement.

If your product will be supplied directly to the customer, assess the material costs of your product to determine whether you can meet the applicable cost-of-components test. This will require engagement with your supply chain to make certain you are obtaining country-of-origin information on your components, as well as identifying what articles are the actual "components" of the product for

cost purposes. Keep in mind that the cost-of-components test is essentially a materials cost test that does not include the costs associated with manufacturing the end product from its various components.

If you are supplying products subject to the strict iron or steel sourcing requirements of Buy America, you should institute a process to obtain so-called “step certifications” confirming each step of the manufacturing process occurred within the United States.

Be sure to educate your sales and purchasing teams to recognize and distinguish among the various types of Buy American or Buy America requirements. That recognition is key to ensuring that your quotes or proposals account for the correct set of requirements and that your purchase orders to suppliers flow down any terms needed to ensure compliance. It also will help your purchasing department identify areas in which you may need to seek out alternative suppliers, to be able to meet some of the domestic content thresholds.

Finally, make sure your sales team understands the risks posed by signing certifications of compliance with domestic content requirements. Buy America compliance is likely to be a growth area in false claims litigation, and inaccurate certifications provide potential fodder to government officials and qui tam relators. If your product does not comply with the applicable requirement, it is critical that you not claim that it does. While waivers of the Buy America requirements may be difficult to come by, it is far better to try to pursue a waiver than to face the headaches that would result from a false certification of compliance.

[1] *These dollar thresholds are subject to adjustment every two years and are scheduled to be adjusted late this year, with the adjusted thresholds to be effective January 1, 2024.*

[2] *This discussion focuses on the requirements for products that would be considered “manufactured products” under BABA. There would be a need to trace the origin of iron or steel in an iron or steel component of a product considered under BABA to be an “iron or steel product.”*

How to Protect Intellectual Property During Product Development

In this article, we discuss critical intellectual property considerations, including patents and trade secrets, for companies engaging in development of key technology. Covered topics will include employment agreements and onboarding processes for new employees, and joint development agreements (JDAs) with third party collaborators.

Today’s high-tech products require a combination of skills across an array of engineering disciplines. For example, producing electric vehicles requires the integration of manufacturing prowess, electrical brilliance, and software genius. As a result, companies constantly collaborate across disciplines, often resulting in relationships with third parties that are often of a dissimilar industry, location, and maturity. Later disputes with these parties over intellectual property can delay or destroy progress, crippling companies while their competitors succeed. This article provides guidance on avoiding such pitfalls.

Put Intellectual Property at the Forefront of Relationships and Engagements

The first step toward effectively protecting intellectual property (IP) (e.g., patents, trade secrets, trademarks, copyrights, etc.) is to raise the issue before development even begins. This applies to both relationships with new employees and new engagements with third parties (e.g., vendors,

suppliers, contractors, etc.). Agreements governing these relationships and engagements should be carefully crafted not only to maintain ownership of IP that existed beforehand (so-called "background" IP) but also to parse out ownership and use of IP that will be developed during the course of the development relationship (so-called "foreground" or "generated" IP). Relationships often change as time goes on, and parties' views on the value of generated IP may evolve during the course of development, so it is typically easier

IP-Conscious On-Boarding of New Employees

New employees bring fresh ideas to a team, but employers should take steps to educate new employees to protect future IP and reduce risks associated with third-party IP. During on-boarding, new employees should be educated as to the different types of IP with examples of how each type of IP is typically generated. This education should also teach new employees to recognize when their future work generates IP and inform them as to the internal processes the employer uses to harvest this IP. One common practice is for employees to expeditiously submit invention disclosures to an internal "invention review committee" that is responsible for selecting which will be pursued in patent applications and which will be kept as trade secrets.

Part of this education should also focus on effective and efficient documentation of new IP. New employees should be encouraged to save and date any information generated during initial brainstorming of IP and to promptly facilitate harvesting of the IP by the employer.

Another critical teaching point involves providing education on standard confidentiality practices for safeguarding IP from non-employees. To the extent that collaboration with a third party is necessary (a point which is discussed in more detail below), employees should be trained to first confirm that proper agreements (e.g., non-disclosure agreements, confidentiality agreements, joint development agreements, etc.) are in place. Ideally, any IP would be harvested before any collaboration occurs, either by filing a patent application, recording new innovations in a trade secret log, and/or modifying existing agreements as needed.

New employees should also be trained to understand their obligations to their former employers, and their ideas should be screened to reduce the risk of such "IP contamination." Such policies can help protect against IP claims from the prior employer, such as those for trade secret misappropriation or breach of confidentiality.

The legal language of employment agreements should also be carefully reviewed on an ongoing and routine basis. For example, employment agreements should be drafted to state that employees "do hereby assign" their IP rights to the employer. The present tense language is critical. Other language can be found insufficient to cement the employer's right to the IP. In addition to keeping legal language up to date, ongoing review of employment agreements will help ensure that they remain focused on the employer's current and future business interests.

Forging Symbiotic Relationships with Third Parties

Engagements with third parties, often arising in the form of joint development agreements (JDAs), should receive similar care and planning. As with any agreement, carefully drafting terms to achieve specific goals while simultaneously mitigating risk is vital. This is especially the case for JDAs involving the development of key technology with dissimilar collaborating parties. When collaborating parties are differently situated (e.g., established OEM vs. budding start-up), differently located (e.g., domestic vs. foreign), or have different commercial goals (e.g., beholden to shareholders or some

particular financial metric), it is imperative to have a carefully crafted JDA that facilitates the creation and protection of key technology.

Defining the Collaboration

As a threshold matter, it is necessary to identify the proper parties involved in joint development efforts. In many instances—even those involving young companies or those new to a particular technological area—multiple separate legal entities can be involved in activities that may yield new intellectual property or require use of existing intellectual property. As a further complication, these legal entities may have obligations to other legal entities. Failing to identify the proper parties could undermine the utility of the JDA. Conducting thorough due diligence is necessary to mitigate risk at this threshold step.

Identification of proper parties can also require an accurate and complete understanding of the scope of work contemplated by the JDA. Specifically, it is important to understand what work will be done and when, who is doing the work, and what IP is expected to be generated. For example, is the work likely to generate entirely new IP, combine existing-but-separate technologies together, integrate existing technology into a new product, or something else? Based on the work to be performed, which party or parties are likely to generate IP?

When completion of the work under the JDA involves use of existing IP of one party, a license may be required by the other party to permit use of the background IP to accomplish the efforts outlined in the JDA scope of work. However, such licenses can extend further into subsequent commercialization of generated IP, such as when use of the background IP is required to use the generated IP. In those circumstances, licensing strategies should ideally be tailored to suit the parties' intended commercial uses without extending further than necessary. For example, the license could permit certain uses of the background IP, such as producing a product embodying the generated IP for a specific third party, while prohibiting other uses, such as producing another product embodying the background IP for a competitor.

Planning for Generated IP

A robust JDA will be tailored to particular varieties of IP that are likely to be generated by development efforts. Whether the work performed under the JDA will create copyrightable work, patentable ideas, trade secrets, or some combination will impact the terms of the JDA. If the generated IP is likely to be patentable, the JDA should contemplate, among other things, who will own the resultant patent rights, how those patent rights will be secured, who pays for the patent application process, and the extent to which those rights can be enforced or licensed.

If the generated IP will be kept as a trade secret, the terms of the JDA should provide for adequate security measures to properly maintain the trade secret according to applicable state law. This can be complicated if the parties are located in disparate geographic locations or if the parties have disparate internal security policies, which may justify opting for patent protection over trade secret protection. Whatever the case, it is prudent to consider what form any generated IP may take so as to be readily equipped to protect it.

In addition to identifying what generated IP is likely to result, it is important to be cognizant of where generated IP will be created and where it will be used. With regard to patents, for example, certain countries may impose restrictions on foreign filing based on where the invention was conceived, an inventor's residency, or an inventor's citizenship. Some jurisdictions may even impose restrictions

on how generated IP can be secured. When possible, companies would be wise to plan ahead for how to address these hurdles.

Establishing Ownership of the Generated IP

To avoid unnecessary complications in procurement and later use of generated IP, a JDA should comprehensively define ownership of generated IP. In most jurisdictions, patent rights in an employee's invention initially belong to the employee. Employers typically gain patent rights to their employee's inventions by employment agreement or assignment. During joint development, when employees from both parties are inventors, both parties will have likely obtained rights in the invention from their respective employees. Without a further agreement, both parties will be joint owners of any resulting patent.

While joint ownership can ensure access to the IP, it can present several administrative or logistical difficulties. For example, when generated IP includes patentable ideas, disagreement between joint owners as to procurement, maintenance, defense, or enforcement of patent rights can materially affect the value or utility of the generated IP. This can be especially true when the jointly developing parties belong to different industries or are affected by different motivations or pressures. In the U.S., for example, each joint owner can use the patent, or sell or license their rights in it, without the approval of the other. Further, all joint owners must consent to any patent infringement suit based on the patent.

For these reasons, when available, sole ownership of generated IP may be preferrable to ensure maximum value and utility of the generated IP. For example, sole ownership more readily enables harvesting IP in a manner that will yield commercially-relevant assets. Risks to the non-owning party can be mitigated by including provisions in the JDA imposing an obligation to diligently prepare IP or by otherwise creating some other mechanism for a non-owner to influence a sole owner's control of the generated IP.

Using the Generated IP

Beyond ownership considerations, a JDA should be crafted to include appropriate provisions to govern use of the generated IP. Typically, JDAs include licenses to generated IP (and background IP) owned by the other party for the duration of the joint development efforts. JDAs may also include restrictions on the use of generated IP by the owning party (whether jointly or solely owned). In some cases, licenses and restrictions can also extend to subsequent commercialization of generated IP. When commercial goals diverge, licenses and restrictions can mitigate risk by permitting only appropriate uses of the generated IP by appropriate parties. Licenses to generated IP should consider implications of subscription-based commercialization models, which has become increasingly popular with the proliferation of software in manufacturing-centric industries.

In the modern technological environment, additional representations and warranties beyond standard IP representations and warranties (e.g., ownership, ability to license, ability to perform work, etc.) can be useful. When software is involved, for example, consider adding to the JDA representations and warranties to ensure the software does not include malware or viruses, does not use (or properly identifies) open-source software, or will be adequately maintained or supported over time. These representations and warranties can protect owners and users of the generated IP alike.

Navigate the Treacherous Waters of Collaborations Carefully

With many important factors to bear in mind, effectively navigating relationships with employees and third parties to develop key technology requires careful consideration and planning. This is especially true in the modern technological environment where collaborating parties may be different in significant ways. Below is a checklist of important considerations for your quick reference.

- Consider when on-boarding of new employees;
- Ensure that an NDA is in place before sharing technical information with a third party;
- Document any relevant IP and file relevant patent applications before sharing technical information with a third party;
- Consider how a JDA will be constructed: - Who are the proper collaborating parties?
    - What work will be performed during the collaboration?
    - What IP is needed by both parties to carry out the collaboration and subsequent commercialization?
    - Which parties will generate IP?
    - What form will that IP likely take?
    - Who will own the IP?
    - Who is responsible for securing rights to the generated IP and how are they held accountable?
    - How can the generated IP be used?
    - What uses of the generated IP should be avoided?
    - Are any additional safeguards needed to protect owner and user of generated IP?

2023 CPSC and FDA Enforcement Trends

With the first half of the year behind us, it is clear that 2023 will be a year of increasing regulatory enforcement. Specifically, in the past few months, the U.S. Consumer Product Safety Commission (CPSC or Commission) and the U.S. Food and Drug Administration (FDA or Agency) have engaged in significant enforcement activity with no sign of slowing down.

For the CPSC—while the Commission continues to partner with the U.S. Department of Justice, pursue litigation, and take unilateral action, this article focuses on a particularly challenging enforcement remedy—civil penalties. Given that the obligation to immediately report consumer product issues “which could create a substantial product hazard” or “unreasonable risk of serious injury or death,” applies to manufacturers, importers, and retailers alike,[1] the CPSC’s new focus on harsh civil

penalties is a universal concern.

The FDA has returned to its normal, onsite facility inspection operations after curtailing those efforts due to the COVID-19 pandemic. The Agency has seemingly shifted its enforcement priorities from COVID-19 related matters to other areas of interest, including domestic and foreign inspections, cosmetics products (following passage of the Modernization of Cosmetics Regulation Act of 2022 (MoCRA) in December), and over-the-counter (OTC) drug products.

While the quantity and severity of enforcement actions continue to rise, manufacturers, distributors, and retailers of CPSC and FDA-regulated products must diligently mitigate the risk of becoming the subject of an enforcement action and stay alert. Now more than ever, it is essential that companies cultivate a culture of compliance that incentivizes internal escalation of consumer reports and establish processes and procedures to assess and act on such reports in a timely manner.

CPSC: Civil Penalties Continue to Rise

The Consumer Product Safety Improvement Act (CPSIA)

Under Section 15 of the CPSIA, a manufacturer, importer, distributor, or retailer of a consumer product within the CPSC's purview must inform the CPSC "immediately" upon the receipt of information that "reasonably supports the conclusion that such product:

1. Fails to comply with an applicable consumer product safety rule or with a voluntary consumer product safety standard upon which the Commission has relied under section 9;

2. Fails to comply with any other rule, regulation, standard, or ban under [the Act] or any other Act enforced by the Commission;

3. Contains a defect which could create a substantial product hazard...; or

4. Creates an unreasonable risk of serious injury or death.[2]

The singular exception to the reporting requirement is if the manufacturer, importer, distributor, or retailer "has actual knowledge that the Commission has been adequately informed" of such defect, failure to comply, or risk.[3] As to the last two circumstances above, neither the CPSIA nor the CPSC's corresponding regulations provide a definitive answer as to when a duty to report to the CPSC arises, but the CPSC generally advises companies, "when in doubt, report."

Civil Penalties: A Multi-Factored Analysis

Effective August 14, 2009, the CPSC increased the maximum civil penalty to $100,000 per violation and $15 million for a related series of violations. Since then, the CPSC has applied regular statutory cost-of-living adjustments.[4] Currently, the maximum penalty is $120,000 per violation and $17.15 million for a related series of violations.[5]

The CPSC weighs several statutory factors in considering a civil penalty. Specifically, "[i]n determining the amount of such civil penalty or whether it should be remitted or mitigated and in what

amount, the Commission shall consider the appropriateness of such penalty to the size of the business of the person charged, including how to mitigate undue adverse impacts on small businesses, the nature, circumstances, extent, and gravity of the violation including, the nature of the product defect, the severity of the risk of injury, the occurrence or absence of injury, and the number of defective products distributed, and such other factors as appropriate."[6] In addition to these statutory factors, the CPSC has also issued guidance that includes additional factors like whether a company has a safety compliance program, a history of noncompliance or economic gain from noncompliance, and whether the company responded to the CPSC's inquiry in a timely and complete manner.[7]

Most CPSC late reporting penalty cases involve allegations that the company should have reported earlier when, among other things, the available information "reasonably supports the conclusion" that a product "contains a defect which could create a substantial product hazard" or the product "creates an unreasonable risk of serious injury or death."[8] The CPSC's guidance notes the following relevant factors—any one of which can result in a finding that a product defect creates a substantial product hazard—pattern of defect, number of defective products distributed in commerce, severity of the risk, or other considerations.[9] The determination of whether a risk is "unreasonable" also involves consideration of several factors, including the product's utility, the nature and extent of the risk, and the availability of alternative designs or products that could eliminate the risk.[10] Information that is helpful in assessing that risk may include expert reports, test data, product liability claims, consumer complaints, quality control data, studies, injury reports, and information from industry or government.[11] In evaluating whether information is reportable, it is important to remember that hindsight is always 20/20.

Civil Penalties in 2023

Last year's predicted trend of increased penalties for failure to timely report has come to fruition in the first half of 2023. Thus far, the CPSC has announced two eight-figure civil penalty settlement agreements—the first for $19,065,000 and the second for $15,800,000. If recent trends continue, the CPSC will exceed all historical norms in terms of the quantity and severity of civil penalties issued to consumer product companies.

The CPSC started 2023 off with a bang, announcing the $19,065,000 Peloton Interactive Inc. settlement— one of the largest penalties in CPSC history—on January 5, 2023. According to the press release and agreement, despite receiving "reports of incidents associated with pull under and entrapment in the rear of the treadmills, including reports of injuries" in December 2018 and continuing into 2019, Peloton did not report the issue to the CPSC until March 4, 2021. By then, "there were more than 150 reports of people, pets, and/or objects being pulled under the rear of the Tread+ treadmill, including the death of a child and 13 injuries, including broken bones, lacerations, abrasions and friction burns."

The CPSC issued a unilateral press release on April 17, 2021, warning consumers to stop using the Tread+ treadmills "after multiple incidents of small children and a pet being injured beneath the machines." Peloton then recalled its Tread+ treadmill shortly thereafter on May 5, 2021. The settlement agreement indicates that the CPSC imposed a penalty for two reasons: knowing failure to immediately report and knowing distribution of recalled products. Thus, because it was premised on two separate charges, the penalty exceeded the statutory maximum.

While the recall remained pending, the CPSC issued a unilateral press release on April 17, 2021, warning consumers to stop using the Tread+ treadmills "after multiple incidents of small

children and a pet being injured beneath the machines." Peloton then recalled its Tread+ treadmill shortly thereafter on May 5, 2021. The settlement agreement indicates that the CPSC imposed a penalty for two reasons: knowing failure to immediately report and knowing distribution of recalled products. Thus, because it was premised on two separate charges, the penalty exceeded the statutory maximum.

Most recently, on May 5, 2023, the CPSC announced the $15,800,000 Generac Power Systems Inc. settlement. The press release indicates that, beginning "in October 2018 and continuing into 2020, Generac received reports of incidents from consumers whose fingers were partially amputated or crushed by the unlocked handle of the portable generator." "By the time Generac filed a report with the Commission, there were five reports of consumers suffering finger amputations while attempting to transport the portable generators, which required hospitalization, surgery, and/or sutures and resulted in permanent disfigurement." Generac recalled its portable generators on July 29, 2021, and the settlement agreement indicates that the CPSC imposed the civil penalty for knowing failure to immediately report.

Notably, in a statement made relating to the Generac penalty, Commissioner Peter Feldman expressed concern about the CPSC's civil penalty structure and highlighted the need for "a consistent methodology" to calculate penalty amounts. The regulations themselves provide some guidance but arguably leave significant room for the Commission to determine penalty amounts. And given the limited history of civil penalties from the Commission, there is not much precedent to which companies can look to assess their exposure. While the other Commissioners and Chair did not expressly echo Feldman's views, Feldman's statement signals that the future may hold some hope for a "more structured and coherent civil penalty regime that provides clear guidance on the types of conduct that will result in maximum fines, as well as the types of conduct that are suited for other types of relief."

FDA: A Return to Normal Operations and a Shift in Enforcement Focus

Domestic and Foreign Inspections Are On the Rise

For the past several years, the FDA has primarily focused its enforcement actions on violations related to the COVID-19 public health emergency (PHE). In 2021, a majority of the warning letters issued by the FDA were in connection with unapproved products marketed with unsubstantiated claims regarding the treatment and prevention of COVID-19. However, in 2022, the Agency shifted its focus to current good manufacturing practice (cGMP) enforcement actions due to the resumption of onsite domestic and foreign inspections, which were temporarily halted in response to the PHE. As a result, the number of warning letters related to inspections likely will continue to increase as the Agency works through a backlog of inspections that were put on hold during the PHE.

As the FDA returns to normal operations, we expect the Agency to continue its enforcement efforts on onsite inspections. Moreover, we may witness an increase in warning letters issued in relation to onsite foreign inspections as the COVID-19 restrictions are lifted. Therefore, both domestic and foreign manufacturers of food, drug, and medical device products regulated by the FDA should ensure compliance with cGMP regulations and should prepare their facilities for upcoming onsite inspections.

Contract Manufacturers Warned for cGMP Violations

Within the past year, the FDA also issued a number of warning letters to contract manufacturers,

which are third-party manufacturers that contract with firms to produce components or products. A majority of these notified contract manufacturers were involved in manufacturing OTC drug products. In all of these warning letters, the FDA stated that it considers "contractors as extensions of the manufacturer" and that these drug products must be manufactured in conformance with cGMP. Thus, contract manufacturers should also ensure that they meet cGMP requirements and routinely evaluate their operations for cGMP compliance. We anticipate the Agency to continue its enforcement efforts on OTC drug products, particularly after the FDA completed the process of posting deemed final order as part of OTC monograph reform under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

FDA Increases Regulatory Oversight of Cosmetic Products

In the near future, we expect the FDA will also focus on cosmetics products due to the recent enactment of MoCRA last December. MoCRA significantly increases the FDA's oversight of cosmetics products. Under MoCRA, cosmetics companies will now be subject to facility registration and product listing requirements, cGMP requirements, serious adverse event reporting and recordkeeping, and safety substantiation.[20] Additionally, MoCRA expands the FDA's enforcement authority by giving the Agency the authority to mandate recalls for cosmetics products.[21] MoCRA also allows the FDA to suspend facility registrations if a cosmetic product manufactured by a facility has a reasonable probability of causing serious adverse health consequences, and the Agency believes other products may be similarly affected.[22] Most of these provisions under MoCRA will take effect on December 29, 2023.[23] We expect that the FDA will shift its attention to manufacturers of cosmetics products in the next year to ensure compliance with MoCRA.

Looking forward, companies subject to FDA regulation should ensure cGMP compliance (if appropriate) and familiarize themselves with the FDA's Manual of Compliance Policy Guides (CPGs). The CPGs "are intended to advise the FDA staff as to the Agency's strategy when assessing and enforcing industry compliance."24 They are regularly updated and serve as a baseline for companies to consider when evaluating compliance with applicable standards and guidance.

[1] *15 U.S.C. § 2064(b).*
[2] *15 U.S.C. § 2064(b).*
[3] *Id.*
[4] *See Pub. L. No. 110-314, §§ 217(a)(1), (4), 122 Stat. 3016, 3058 (2008).*
[5] *See 86 Fed. Reg. 68,244 (Dec. 1, 2021).*
[6] *15 U.S.C. § 2069(c).*
[7] *See 16 CFR Part 1119.*
[8] *15 U.S.C. § 2064(b).*
[9] *16 C.F.R. § 1115.12(g); see also United States v. Spectrum Brands, Inc., 218 F. Supp. 3d 794, 820-21 (W.D. Wis. 2016), aff'd, 924 F.3d 337 (7th Cir. 2019) (rejecting defendant's argument that no duty to report arose because "none of the reported injuries rose to any particular level of seriousness").*
[10] *16 C.F.R. § 1115.6(b).*
[11] *16 C.F.R. § 1115.6(a).*
[12] *See generally Consol. Approps. Act, 2023, Pub. L. 117-328, Division FF, Title III, Subtitle E – Cosmetics, sec. 3501-3508, 136 Stat. 4459 (2022).*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

Terminating Reseller Relationships Amidst the Network-Consolidation Trend: What Manufacturers Need to Know

Unwinding or outright terminating reseller relationships is a regular part of most manufacturers' businesses when they use independent reseller networks to get their products into the hands of end users. For some, the difficult decision to terminate a reseller may come up once every few years, but for others it recurs with far more frequency and often bogs down manufacturers' sales staff and senior management, who otherwise could focus on more accretive activities. The question of whether to terminate a reseller can present itself for any number of reasons—poor sales performance, a breach of the parties' reseller contract, reseller insolvency, or default on payment obligations, etc. But with increasing frequency over the last decade, the termination question is being triggered by a trend that has swept the United States reseller market no matter the industry or equipment: reseller consolidation. How to handle terminations in the wake of reseller consolidation is the primary focus of this article; but no matter why you are considering a reseller termination, the "Tips on Evaluating Terminations" detailed below provide important food for thought that every manufacturer should consider before making the decision to terminate.

For many manufacturers, reseller network consolidation and restructuring are consciously adopted business strategies, and there are often good reasons to focus product resale efforts through a handful of high-performing, sophisticated resellers—or, perhaps, through a manufacturer's own capable direct sales staff. For other manufacturers, the prospect of network consolidation or restructuring is not a voluntarily adopted strategy. Instead, it's the result of an increasing trend in large resellers pursuing acquisitions of peer resellers within a manufacturer's network to grow their territorial reach.

In either instance, there are obvious benefits to the consolidation trend. Larger resellers offer a predictable product and may be on stronger financial footing, have more refined marketing tools, and are better able to predict the needs of customers. The same is usually true of a manufacturer's direct sales staff, who are usually better funded, better trained, and more conversant on the manufacturer's entire product portfolio.

But there also are challenges that come with network consolidation and restructuring. Larger resellers mean a consolidation of risk in a reseller with more leverage. That problem is amplified when a manufacturer's network includes a handful of large resellers. Although some problems evolve over time, many are (or should be) obvious to manufacturers beforehand.

This is not to say all consolidation is bad, which is why many manufacturers consciously choose to consolidate their networks through restructuring. The key, of course, is for manufacturers to navigate network consolidation and restructuring in compliance with their contractual and statutory obligations to their resellers, while also ensuring their business interests are preserved, and their business goals are achieved as effectively as possible.

For consolidation that was not of their own choosing, this means separating the wheat from the chaff before the consolidation event – typically, the merger or acquisition – actually happens. By doing this, manufactures can maintain control of their networks and, by extension, their brands. For voluntary consolidation and restructuring, this means consolidating your reseller network in ways that comply with controlling law and contractual obligations to avoid unnecessary litigation exposure or, in the worst circumstances, an order enjoining the manufacturer from consolidating its network through the removal of one or more resellers. These efforts can be time consuming (and require substantial advanced planning) but taking the time to ensure consolidation is handled correctly will save

manufacturers significant time and expense in the future (whether in litigation or otherwise).

Evaluating In-Network Reseller Acquisitions and Transfers of Control

Even where a manufacturer does not proactively adopt a strategy of network consolidation, the manufacturer typically still can (and should) inject itself into the consolidation process. Most state laws allow manufacturers who wish to weigh in on the sale of a reseller's business to vet the proposed acquirer before beginning a long-term resale relationship with it. Exercising this control begins with the process of evaluating which transfers to approve and which not to.

The most important consideration in approving or denying a transfer is ensuring that your reseller agreement gives you the right to approve a transfer. It's hard to exercise control if you didn't grant yourself the right to do so

Once you have the right memorialized, the next step is to check the applicable state's distributor/dealer law. Such laws typically restrict a manufacturer's right to approve a transfer of control but do allow for a denial under appropriate circumstances. Some common features of these laws include:

- Notice of proposed transfer from the reseller, to which the manufacturer must respond by either approving the transfer or denying it (typically with the grounds for denial specified). Some states specify the form of the notice or specify the information that must be exchanged between the parties as part of the notice process.

- Typically, a manufacturer must respond to a proposed transfer within a certain timeframe following the proposal (60 days is common). Be aware that some states specify that a proposed transfer is deemed approved if not rejected in that timeframe.

- In many states, a manufacturer may not "unreasonably" withhold consent. (Additionally,

- §or alternatively, the manufacturer may not prevent

- the reseller from obtaining fair and reasonable compensation for the value of the business.) Whether or not a rejection is "reasonable" is often determined by looking at criteria or qualifications normally required of existing or prospective resellers. Additional considerations include whether the transfer would be " substantially detrimental" to the manufacturer and whether the manufacturer's decision was "arbitrary."

- Some states specify factors that may not be considered in evaluating a transfer, or they specify factors that may be considered but which standing alone are insufficient grounds for rejecting a transfer.

Be aware that some states distinguish between transfer of reseller's business as a whole, the assets of the reseller's business, and partial ownership interests in the reseller's business, and that a rejection can give the reseller the right to file a lawsuit to challenge the manufacturer's decision. The rights bestowed, however, are upon your reseller, not the party to which they are proposing to

transfer the business.

Tips on Evaluating Terminations

For manufacturers considering termination because of an untenable reseller transfer like the one described above, or for manufacturers considering terminating a reseller for any other reason (including, perhaps, a desire to consolidate their reseller network,), there are both practical and legal issues to consider.

The choice to terminate a reseller can be a difficult one. Manufacturers must consider not only the business consequences of a termination but also the legal risks that materialize with a botched termination. There are a number of practical steps that manufacturers can take to both increase the likelihood of a successful termination and reduce their exposure to the uncertainty, distraction, and expense of litigation.

First, manufacturers must ask themselves a threshold, but admittedly abstract, question about the termination itself: does it pass the fairness test? As you build your rationale for terminating a reseller, consider what a judge or jury might say in response to your case for termination. Think critically about whether your answers to questions like the following will present your decision in a good light before the judge or jury.

- Are you unfairly singling out this particular reseller (e.g., did your other resellers consolidate without your objection)?
- Are you dumping this reseller for reasons that the applicable statutes deem legitimate (i.e., for “cause”), or is it for the sole reason that you’d prefer a different reseller—or your direct sales team—to handle the territory in question?
- Do you have a uniform process in place for evaluating your reseller’s performance under your agreements or any proposed transfers of your reseller’s business?

These optics matter. Most states require “good cause” to terminate a reseller, and although different states have different standards for what constitutes “good cause,” it will always be more than just a contractual right to terminate or a business goal of network consolidation divorced from your reseller’s performance under your contract. You will likely need to demonstrate that you have “good cause” at some point before the termination is complete, so make sure that you have your story straight and it passes the fairness test before you initiate a termination.

Second, get your termination notice right. Make sure you know how you are supposed to notify your reseller under both your contract and any relevant state statute. You may need to allow time to cure a defect. There may be a waiting period. You may have to include your justification for termination in the notice. Any or all of these may be requirements for you to provide proper notice to a reseller, and each of them could form a basis for legal liability if disregarded. Standing alone, a defective notice can effectively nullify your termination (and subject you to liability under relevant state statutes) even if you have “good cause” to move forward with the termination.

Third, do not sugarcoat your termination notice, and do not rely on things you cannot substantiate—be direct and honest. Rely on the facts and circumstances within the reseller’s control to justify your

decision. Take an interest in the details. How a difficult message is conveyed, and by whom, can make a big difference in how the message is received. Having lawyers send a termination notice may signal that you're expecting a fight in a way that delivering a sincere letter from a business partner may not. Making termination easy to hear and digest for your reseller can reduce the likelihood of a lawsuit.

Fourth, do not concede the applicability of any state statute. There can be many reasons a given state dealer/ distributor statute does not afford a reseller protection from termination. Your termination notice will be "Exhibit A" to any terminated reseller's complaint filed against you, and a concession that a particular state statute applies may forestall your later attempt to argue the statute is inapplicable.

Last, give your reseller a reason to go away quietly. As a manufacturer, there are ways that you can ease the transition a terminated reseller will experience. Are you able and willing to repurchase inventory regardless of whether an obligation exists? Maybe you can waive a contractual non-compete clause without serious consequences. Even providing a lump sum payment to a reseller may give them an incentive to avoid litigation, and it may be cheaper in the long run. These efforts can go a long way toward ending a business relationship on good terms and avoiding unnecessary acrimony.

Terminating a reseller requires careful planning and precise execution to avoid practical and legal pitfalls. These tips are meant as both an aid and a warning. Manufacturers who intend to terminate a reseller need to approach the situation strategically to avoid the risk of ill will or, worse, a lawsuit.

Top Environmental Issues Facing the Manufacturing Sector: The EPA Tackles Climate Change and Emerging Contaminants

Since Joe Biden's election to the presidency in 2020, the United States Environmental Protection Agency (EPA or the Agency) has actively worked to implement a regulatory agenda that focuses on two core goals: (1) addressing the effects of climate change, and (2) reducing exposures to emerging contaminants of concern such as per- and polyfluoroalkyl substances (PFAS). Over the past year, EPA has continued its rulemaking and enforcement efforts in these areas, and we expect the trend will continue through 2023.

EPA's focus is particularly notable because, unlike some of the Agency's past priority areas, the emission of greenhouse gases and the manufacture and use of PFAS are not limited to small or discrete sectors of regulated industry; rather, the potential breadth of EPA's regulatory and enforcement efforts is far reaching. EPA's proposed climate change regulations will affect a variety of regulated entities in the manufacturing space, including manufacturers in the automotive and equipment industries, commercial refrigeration, air conditioning, heating and cooling, and many other industries.1 Similarly, PFAS have been used in a wide variety of industries, including production of organic chemicals, plastics/synthetic fibers, electrical components, textiles, and pulp/paper/paperboard, as well as in leather tanning/finishing, metals finishing/electroplating, plastics molding, and paint formulating, among others. As such, the imposition of restrictions on the use and disposal of PFAS are likely to have broad implications. Now more than ever, manufacturing companies are facing an increasingly complex web of environmental regulations and an EPA that has demonstrated willingness to enforce them.

EPA's Avalanche of Air Rules to Address Climate Change and Other Emissions

EPA has been busy issuing a number of watershed rules and proposals under the Clean Air Act (CAA) and other authorities related to air emissions and greenhouse gases. Many of the EPA rules and proposals have specifically targeted vehicle emissions and are likely to have significant impacts on American vehicle manufacturers and the entire automotive supply chain.

On January 24, 2023, the EPA published final rules for emission standards for heavy-duty highway vehicles and engines, including heavy-duty trucks and other vocational vehicles (such as fire trucks), recreational vehicles, coach buses, and other over-the-road vehicles like cement trucks, beginning with the 2027 model year. These standards became effective on March 27, 2023.2 This final rule continues the Agency's aggressive regulation of mobile source emissions. While the final rule focuses primarily on nitrogen oxide (NOx) emission standards, the Agency anticipates that the final rule will result in significant reductions in not only NOx but secondary pollutants such as fine particulate matter (PM2.5) and ozone.

Building on these standards, on April 12, 2023, EPA proposed two aggressive new mobile source regulations limiting tailpipe emissions: one targeting light- and medium-duty vehicles and one targeting heavy-duty highway vehicles.3 If adopted, manufacturers would need to quickly scale up zero-emission vehicle production, such as electric vehicle (EV) production, in order to meet the proposed rules' requirements. The proposed rules would have a significant impact on the entire automotive supply chain as well as on logistics suppliers, and expedite the need for aggressive investments in charging stations and upgrades to the transmission grid nationwide to accommodate the increased demand for EV charging capacity. The proposals target not only criteria pollutant emissions like NOx and PM from light and medium duty vehicles, but also greenhouse gas emissions from heavy-duty vehicles beginning with the 2027 model year. Comments on these two proposals are due in June and July 2023 with hundreds of interested stakeholder already weighing in on the proposals or participating in the EPA hearings on the proposals.

In addition to these proposed and final rulemakings specifically aimed at vehicle emissions, EPA issued a proposed rule at the end of 2022 under the American Innovation and Manufacturing (AIM) Act to address the impact of hydrofluorocarbons (HFCs), which are potent greenhouse gases and ozone-depleting substances commonly used in a variety of materials such as aerosols, foams, and refrigerants.4 Generally, the proposal prohibits the manufacture and import of products containing restricted HFCs by January 1, 2025, and prohibits the sale, distribution, and export of products containing restricted HFCs by January 1, 2026. If finalized as drafted, the rule may require manufacturers to transition from HFC-based systems sooner than previously anticipated.

On January 6, 2023, EPA also proposed to lower the primary National Ambient Air Quality Standard (NAAQS) for fine/inhalable particulate matter (PM2.5).5 EPA is proposing to lower the primary NAAQS PM2.5 emission standard from 12 micrograms per cubic meter (µg/m3) to between nine and ten µg/m. The new standards, if issued as proposed, would likely result in many areas of the country being designated as in nonattainment with the new standards. This, in turn, could trigger significant new costs and control requirements for manufacturing facilities with air permits in those new nonattainment areas.

Each of these rules and proposals have the potential to have significant impacts on the manufacturing industry in terms of forcing redesign of products, requiring investment in research and development, and increasing permitting and other regulatory compliance burdens. EPA shows no signs of slowing down in its rulemaking activities, and if the Agency's current actions areany indication, we expect there to be more proposals related to air emissions from the Agency throughout the remainder of the year with similar implications for the manufacturing industry.

An Emerging Regulatory and Enforcement Framework for PFAS

Regulatory Efforts

In recent years, EPA's regulatory framework for regulating PFAS has lagged significantly behind individual state efforts, as state legislatures across the country have moved quickly to restrict the intentional addition of certain PFAS in consumer goods and to promulgate binding standards to address PFAS contamination in soil and groundwater. However, in October 2021, EPA announced its "strategic roadmap" for regulating PFAS, which prioritized a wide variety of targeted rulemakings and data collection efforts. The roadmap identified specific industries as particular targets for PFAS regulation, including plastics/synthetic fibers manufacturing, plastics molding, metal finishing/electroplating, electrical component manufacturing, and pulp/paper/paperboard manufacturing, among others. However, given the number of other industries that rely on these industries to supply materials for manufacturing, the impact of implementation of the strategic roadmap is expected to be much broader. Over the past year, EPA has taken significant steps toward developing a national framework for regulation consistent with this roadmap.

Proposed Listing of PFOA and PFOS as CERCLA Hazardous Substances

In August 2022, EPA proposed listing two individual PFAS – perfluorooctanoic acid (PFOA) and perfluorooctane sulfonic acid (PFOS) – as hazardous substances under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA). This represents a watershed moment in PFAS regulation. If the proposed rule is finalized as expected, it will trigger new reporting obligations for regulated industry and impose liability for both historical and future releases. Among other impacts, EPA's action is likely to draw increased scrutiny on current and closed Superfund sites for these largely previously uninvestigated chemicals. In response, industry groups have pushed for relatively limited CERCLA liability exemptions for select "downstream" regulated entities such as publicly-owned treatment works and airports. However, Congress would need to amend CERCLA to establish a statutory basis for any exemptions before EPA could employ them, and the likelihood of such an amendment is murky at best.6 As things stand in the current proposal, any manufacturing entity with liability at any current or formerly contaminated site, even sites having already received closure, could be subject to PFOS or PFOA investigation or cleanup obligations or third party claims under CERCLA's strict, joint-and-several liability.

Even as EPA's proposed listing remains pending, regulated entities have noted an uptick in requests issued by EPA under Section 104(e) of CERCLA (42 U.S.C. § 9604(e)(2)) relating to current and past use of PFAS at existing Superfund sites. Under Section 104(e), EPA has authority to request information from any person about any release of a "hazardous substance" or a "pollutant or contaminant" to determine whether a response action is appropriate. As noted above, although no PFAS are yet listed under CERCLA as a "hazardous substance," EPA has taken the position that both PFOS and PFOA are CERCLA pollutants and/or contaminants, and thus within the purview of the Agency's 104(e) authority. The CERCLA 104(e) requests are often drafted extremely broadly and many manufacturers report needing to expend significant resources to collect and cull responsive information, even for sites they may no longer own or operate. And CERCLA 104(e) requests are similar to litigation interrogatories in that while a party may lodge objections when responding to EPA's requests, a lack of response (or a deficient response) risks civil penalties.

EPA's robust PFAS information-gathering naturally raises the question of what the Agency intends to do with the data about PFAS at these sites. In addition to potentially providing the basis for additional investigation and response actions at existing Superfund sites, it is possible that EPA could

incorporate the data into its public tools that map potentially contaminated facilities, such as EJScreen.

Proposed TSCA Amendments

Another key element of EPA's strategic roadmap for PFAS involves changes to regulations affecting the manufacture and importation of PFAS substances themselves. This year, EPA has proposed to remove certain exemptions for PFAS under the Toxic Substances Control Act (TSCA) New Chemicals Review Program (NCRP). In brief, TSCA requires manufacturers to submit notice to EPA before beginning to manufacture or import a "new chemical substance" (defined as any chemical not currently on the TSCA Inventory) so EPA can assess whether the substance is "likely to present an unreasonable risk" of injury to health or the environment before the substance is commercialized. However, the NCRP establishes a low-volume exemption (an LVE) to this premanufacture notice requirement, and many manufacturers have been relying on this exemption as it pertains to PFAS. In the past several years, EPA has taken the informal position that new PFAS substances are ineligible for LVEs and another type of exemption under the statute (low release and exposure, or "LoREX" exemptions), and has encouraged manufacturers to voluntarily cancel the more than 600 LVEs for PFAS that EPA has approved.

In May 2023, EPA released a proposed rule amending its TSCA regulations to codify its position that certain PFAS will no longer qualify for LVE and LoREX exemptions on a go-forward basis (i.e., the limitations do not apply retroactively). If finalized as proposed, this rule would require many manufacturers and importers to reevaluate applicability of PMN provisions to their products and supply chains.

A notable aspect of EPA's proposed rule is that it does not define the term "PFAS" as broadly as some other regulatory definitions. However, the proposed definition does include PFAS commonly known as GenX substances, as well as many fluoropolymers. We expect that the proposed definition will generate significant comment from both industry groups (who will likely favor it) and public interest groups (who will likely push for the broader definition currently used by some states).

In addition to this change to the NCRP, EPA has also proposed broad reporting and recordkeeping requirements under TSCA Section 8(a). EPA's stated intent is to enable EPA to better characterize the sources and quantities of PFAS manufactured in or imported into the United States. This rule, if finalized as proposed, would require regulated entities to provide detailed reports about the entities usage of PFAS dating back to January 1, 2011, well before PFAS were a "hot topic" in many corners of the manufacturing sector. The rule as proposed does not contain de minimis exemptions, nor does it contain exemptions for "articles" (like some other TSCA provisions). Because of its sweeping scope, industry vociferously challenged EPA's economic impact analysis for the implementation of the rule. It is believed that in response to this and its own internal revised cost estimates, EPA has delayed finalization of the rule to revisit its scope. Manufacturers would be wise to keep abreast of this rulemaking as it has the potential to require significant resources to comply with when finalized.

Enforcement Efforts

As EPA continues to expand its regulatory authority for PFAS, it has also ramped up PFAS enforcement efforts under its existing statutory authority. In January 2023, the Agency released a proposed updated draft of its National Enforcement and Compliance Initiatives (NECI), which EPA states are established to "focus resources on serious and widespread environmental problems where federal enforcement can make a difference." For the upcoming 2024-2027 four-year review cycle,

EPA proposed a new enforcement initiative: addressing PFAS contamination. The proposed initiative states that EPA will develop a CERCLA enforcement discretion and contribution protection settlement policy that may prioritize enforcement efforts against certain regulated entities while exempting others; however, EPA has not yet provided any details. Industry stakeholders have raised concerns about adding PFAS enforcement to the NECI, noting that the proposal appears to treat all PFAS the same, regardless of demonstrated health effects.

To date, EPA's PFAS enforcement actions have had an element of novelty. For example, in April the Agency filed its first-ever enforcement action under the Clean Water Act (CWA) to address PFAS discharges from an industrial facility in West Virginia. In the action, EPA alleges that the facility is exceeding limits for certain PFAS contained in a National Pollutant Discharge Elimination System (NPDES) permit issued by the state agency to the facility in 2018. The action comes barely a year after EPA issued guidance to states authorized to administer NPDES programs on how to incorporate PFAS into wastewater and stormwater permits issued under the NPDES program. The guidance encourages states to identify known or suspected sources of PFAS via sampling methods, and then use their pretreatment permitting authority to add Best Management Practices ("BMPs") and technology-based treatment requirements to NPDES permits to address PFAS discharges.

It is especially noteworthy that EPA's recent CWA enforcement action was well-publicized, suggesting that EPA will continue to prioritize this type of action to encourage more conservative handling of potential PFAS discharges by regulated industry. EPA's eagerness to showcase its enforcement efforts also could be read as EPA signaling to states to ramp up PFAS-related enforcement of the NPDES programs within their jurisdictions.

[1] *Not to mention EPA's recent proposal aimed at greenhouse gases in the fossil fuel-fired power plant sector which could have sweeping implications for that industry and may have downstream effects on the cost of energy used by manufacturers. New Source Performance Standards for Greenhouse Gas Emissions From New, Modified, and Reconstructed Fossil Fuel-Fired Electric Generating Units; Emission Guidelines for Greenhouse Gas Emissions From Existing Fossil Fuel-Fired Electric Generating Units; and Repeal of the Affordable Clean Energy Rule, 88 Fed. Reg. 33240 (May 23, 2023).*

[2] *Control of Air Pollution from New Motor Vehicles: Heavy-Duty Engine and Vehicle Standards 86 Fed. Reg. 4296 (January 24, 2023).*

[3] *Greenhouse Gas Emissions Standards for Heavy-Duty Vehicles— Phase 3, 88 Fed. Reg. 25926 (Apr. 27, 2023); Multi-Pollutant Emissions Standards for Model Years 2027 and Later Light Duty and Medium-Duty Vehicles, 88 Fed. Reg. 29184 (May 5, 2023).*

[4] *Phasedown of Hydrofluorocarbons: Restrictions on the Use of Certain Hydrofluorocarbons Under Subsection (i) the American Innovation and Manufacturing Act of 2020, 87 Fed. Reg. 76738 (Dec. 15, 2022).*

[5] *Reconsideration of the National Ambient Air Quality Standards for Particulate Matter, 88 Fed. Reg. 5558 (Jan. 27, 2023).*

[6] *As noted below, EPA has the discretion to issue enforcement guidance under CERCLA, though that does not have the binding force of law and is subject to change at any time.*

SEC Final Rules Mandating Compensation Clawbacks in Connection with a

Restatement or Revision

In October 2022, the SEC adopted a rule requiring the NYSE and Nasdaq to extend the application of incentive compensation clawbacks first mandated by the Sarbanes Oxley Act of 2002 (SOX) to the compensation of all company executives, not just the CEO and CFO as under the original SOX rule, where a company's financial statement has to be restated or revised to correct a material error. Under this new SEC tule, clawbacks will be required even if the material error was not the result of "misconduct".

On February 22, 2023, both the NYSE and Nasdaq proposed new listing standards requiring issuers to adopt, implement, and enforce written clawback policies directing the recovery of erroneously awarded executive incentive compensation. On June 9, 2023, the SEC approved these listing standards, effective as of October 2, 2023, which will require publicly traded manufacturing companies to have these policies and related procedures in place by December 1, 2023.

Publicly traded manufacturers and their audit and compensation committees, executive officers, and outside advisors should prepare now to deal with the significant implications of new listing standards. Even those manufacturing companies that have written clawback policies in place currently will likely need to expand those policies to comply with these new standards.

Executive Summary

- The rules will require the clawback policy to be triggered when an issuer is required to prepare an accounting restatement due to material noncompliance with any financial reporting requirement.

- Triggering restatements will include both so-called "Big R" and "little r" restatements. That is, they will include any required accounting restatement to correct an error in previously issued financial statements that is material to the previously issued financial statements, or that would result in a material misstatement if the error were corrected in the current period or left uncorrected in the current period.

- The policy will apply to incentive-based compensation received by current or former executive officers during the three completed fiscal years immediately preceding the date on which the issuer is required to prepare the accounting restatement.

- It will not be relevant whether there is any fault on the part of the executive officer who received the compensation or whether the officer was involved in preparing the financial statements subject to the restatement.

- Incentive-based compensation subject to the clawback will include compensation that is granted, earned, or vested based wholly or in part upon the attainment of a financial reporting measure. A " financial reporting measure"is a measure determined and presented in accordance with the accounting principles used in preparing the issuer's financial statements, any measures that are derived wholly or in part from such measures, and stock price or total shareholder return (TSR). Equity awards that vest based solely on continued employment, and that are not granted on the basis of achieving a financial performance goal, will not be subject to the policy.

- The amount required to be clawed back will be the excess of the amount of incentive-

based compensation the executive officer actually received over the amount the executive officer would have received based on the restated numbers, determined on a pre-tax basis. Where the incentive compensation is based on stock price or TSR, reasonable estimates can be used to calculate the excess amount.

- The issuer will be required to enforce the clawback policy except in narrowly defined exceptional circumstances where the direct expense paid to a third party to enforce the policy would exceed the amount of the recovery, the recovery would be illegal under home country law, or the recovery would likely cause an otherwise tax-qualified, broad- based retirement plan to fail to meet certain tax qualification requirements.

- The issuer will not be allowed to indemnify officers or pay for insurance to cover amounts that are clawed back.

- The issuer will need to file its clawback policy as an exhibit to its annual report and to disclose certain information about its enforcement of the clawback policy in proxy statements and Forms 10-K in specified circumstances.

- Two new checkboxes will be added to the cover page of Form 10-K relating to whether the financial statements included in the Form 10-K reflect the correction of an error to previously issued financial statements and whether any of those error corrections are restatements that require a recovery analysis of incentive-based compensation received by executive officers.

Required Elements of the Clawback Policies

The clawback policies mandated by the new Rule 10D-1 will have to meet various requirements as to their scope and application, as summarized below.

1. Type of Restatement Triggering Recovery of Compensation. The clawback policy will be triggered when an issuer is required to prepare an accounting restatement due to the material noncompliance of the issuer with any financial reporting requirement under the securities laws. Triggering restatements will include any required accounting restatement to correct an error in previously issued financial statements that is material to the previously issued financial statements, or that would result in a material misstatement if the error were corrected in the current period or left uncorrected in the current period. The SEC staff has provided guidance on making materiality determinations in Staff Accounting Bulletin No. 99, Materiality, and Staff Accounting Bulletin No. 108, Considering the Effects of Prior Year Misstatements when Quantifying Misstatements in Current Year Financial Statements.

   Rule 10D-1 does not define “accounting restatement” or “material noncompliance” as existing accounting standards and guidance set forth the meaning of those terms. Under current accounting standards, certain changes would not constitute an error correction, including the following: retrospective application of a change in accounting principle; retrospective revision to reportable segment information due to a change in internal organization structure; retrospective reclassification due to a discontinued operation; retrospective application of a change in reporting entity; retrospective

adjustment to provisional amounts in connection with a prior business combination; and retrospective revision for stock splits, reverse stock splits, stock dividends, or other changes in capital structure.

2. Individuals Covered. The clawback policy will be required to apply to any individual who served as an executive officer at any time during the performance period that applied to the incentive-based compensation that the individual received. Accordingly, the policy will apply to both current and former executive officers.

   Rule 10D-1 uses a definition of “executive officer” similar to the definition under Rule 16a-1(f) of the Securities Exchange Act of 1934 (Exchange Act), rather than the definition of “executive officer” under Rule 3b-7 under the Exchange Act. This definition generally includes the issuer’s president; principal financial officer; principal accounting officer (or, if none, the controller); any vice-president in charge of a principal business unit, division, or function; and any other officer who performs a policy-making function, or any other person who performs similar policy-making functions.

3. Definition of “Incentive-Based Compensation” Subject to Recovery. The clawback policy will be required to apply to "incentive-based compensation," which is defined as compensation that is granted, earned, or vested based wholly or in part upon the attainment of a "financial reporting measure." "Financial reporting measure" is defined as a measure that is determined and presented in accordance with the accounting principles used in preparing financial statements, and any measures derived from such measures. This includes non-GAAP financial measures and other measures not presented in the financial statements or SEC filings. "Financial reporting measure" is also defined to include stock price and total shareholder return (TSR).

   The SEC noted that "incentive-based compensation" is to be determined in a principles-based manner so that new forms of compensation and new measures of performance will be captured. The SEC provided in the adopting release a non-exhaustive list of examples of "incentive compensation":

   - Non-equity incentive plan awards that are earned based wholly or in part on satisfying a financial reporting measure performance goal;
   - Bonuses paid from a “bonus pool,” the size of which is determined based wholly or in part on satisfying a financial reporting measure performance goal;
   - Other cash awards based on satisfaction of a financial reporting measure performance goal;
   - Restricted stock, restricted stock units, performance share units, stock options, and stock appreciation rights (SARs) that are granted or become vested based wholly or in part on satisfying a financial reporting measure performance goal; and

- Proceeds received upon the sale of shares "acquired through an incentive plan that were granted or vested based wholly or in part on satisfying a financial reporting measure performance goal.

The SEC also provided examples of compensation that is not “incentive-based compensation”:

- Salaries (unless an increase is based wholly or in part on satisfying a financial reporting measure performance goal);
- Discretionary bonuses not paid from a “bonus pool” determined by satisfying a financial reporting measure performance goal;
- Bonuses paid solely upon satisfying one or more subjective standards or completion of a specified employment period;
- Non-equity incentive plan awards earned solely upon satisfying strategic or operational measures; and
- Equity awards for which the grant is not contingent on achieving any financial reporting measure performance goal and vesting if contingent solely upon continued employment or attaining nonfinancial reporting measures.

4. Time Periods Covered. The clawback policy will apply to incentive-based compensation "received" during the three fiscal years (and certain transition periods resulting from a change in fiscal year) preceding the date on which the issuer is required to prepare the accounting restatement. Compensation will be deemed "received" when the performance condition is satisfied, even if the compensation is not actually paid or granted until a later date. The SEC noted in the adopting release that the date of receipt of the compensation depends on the terms of the award and provided the following examples:

    - If the grant of an award is based, either wholly or in part, on satisfaction of a financial reporting measure performance goal, the award would be deemed received in the fiscal period when that measure was satisfied;
    - If an equity award vests only upon satisfaction of a financial reporting measure performance condition, the award would be deemed received in the fiscal period when it vests;
    - A non-equity incentive plan award would be deemed received in the fiscal year that the executive officer earns the award based on satisfaction of the relevant financial reporting measure performance goal, rather than a subsequent date on which the award was paid; and
    - A cash award earned upon satisfaction of a financial reporting measure performance goal would be deemed received in the fiscal period when that measure is satisfied.

The date on which the issuer is required to prepare the accounting restatement will be the earlier of (a) the date the board, committee, or authorized officer concludes, or should reasonably have concluded, that the issuer is required to prepare an accounting restatement due to material noncompliance with any financial reporting requirement or (b) the date a court, regulatory, or other legally authorized body orders a restatement. The SEC noted in the adopting release that the determination an issuer is required to prepare an accounting restatement may occur before the precise amount of the error has been determined. For an accounting restatement for which an issuer is required to file an Item 4.02(a) Form 8-K, the conclusion that the issuer is required to prepare an accounting restatement is expected to coincide with the occurrence of the event disclosed in the Form 8-K. Furthermore, in determining when there should reasonably have been a conclusion to prepare an accounting restatement, an issuer would have to consider any notice it may receive from its auditor that previously issued financial statements contain a material error.

5. Amount of Recovery. The amount of the recovery will be the amount by which the incentive-based compensation the executive officer actually received exceeds the amount the executive officer would have received based on the restated numbers. The amount of the recovery will be calculated on a pre-tax basis. Where the incentive-based compensation is based on stock price or TSR, reasonable estimates can be used to calculate the excess amount, but the issuer must maintain documentation of the determination of the reasonable estimate and provide the documentation to its national securities exchange or association.

   The SEC noted that the definition of erroneously awarded compensation is intended be applied in a principles-based manners but provided the following guidance:

   For cash awards, the erroneously awarded compensation is the difference between the amount of the cash award (whether payable as a lump sum or over time) that was received and the amount that should have been received applying the restated financial reporting measure.

   - For cash awards paid from bonus pools, the erroneously awarded compensation will be a pro rata portion of any deficiency that results from the aggregate bonus pool that is reduced based on applying the restated financial reporting measure.

   - For equity awards, if the shares, options, or stock appreciation rights (SARs) are still held at the time of recovery, the erroneously awarded compensation will be the number of such securities received in excess of the number that should have been received applying the restated financial reporting measure (or the value of that excess number). If the options or SARs have been exercised, but the underlying shares have not been sold, the erroneously awarded compensation will be the number of shares underlying the excess options or SARs (or the value thereof).

   Amounts recovered from the executive under Section 304 of the Sarbanes-Oxley Act of 2002 may be credited as a reduction in the amount required to be recovered under the Rule 1OD-1 clawback, but the adopting release states that recovery under Rule

1OD-1 will not preclude recovery under the Sarbanes-Oxley Act to the extent any applicable amounts have not been reimbursed to the issuer.

6. Recovery Mandatory Unless Impracticable for One of Three Reasons.Recovery of incentive-based compensation subject to the clawback will be mandatory unless the issuer's compensation committee comprising independent directors, or a majority of independent directors in the absence of a committee, determine that recovery is "impracticable" for one of the following three reasons:

    - The direct expense paid to a third party to assist in enforcing the policy would exceed the amount to be recovered. This basis for impracticability would be available only after the issuer has made a reasonable attempt to recover compensation, documented such attempt, and provided the documentation to its national securities exchange or association.

    - Recovery would violate home country law where the law was adopted prior to the date of the final rule's publication in the Federal Register. This basis for impracticability would be available only after the issuer has obtained an opinion of home country counsel as to the violation and provided the opinion to its national securities exchange.

    - Recovery would likely cause an otherwise tax-qualified, broad-based retirement plan to fail to meet the requirements of Section 401(a)(13) or Section 411(a) of the Internal Revenue Code of 1986, as amended.

    Boards will be permitted to exercise discretion, subject to reasonable restrictions, as to the means of recovery.

    The recovery, however, must be effectuated reasonably promptly. The SEC rule does not define "reasonable promptness," but the Commission’s expectation is that the issuer and its directors will pursue the most appropriate balance of cost and speed in determining the appropriate means to seek recovery in light of their fiduciary duty to safeguard the assets of the issuer, taking into account the time value of money. The SEC also noted that an issuer may be acting reasonably promptly in establishing a deferred payment plan that allows repayment as soon as possible without unreasonable economic hardship to the executive officer.

Clawback Policy Disclosures

The final rules include several disclosure requirements relating to the clawback policy. An issuer's compliance with the disclosure requirements will be an element of the listing standards.

1. Filing of Clawback Policy. The issuer will need to file the clawback policy as an exhibit to its annual report on Form 10-K.

2. Proxy Statement/Annual Report Disclosures. The rule amends Item 402 of Regulation S-K to require disclosure by listed issuers if at any time during or after the last

completed fiscal year the issuer was required to prepare an accounting restatement that required recovery of excess incentive-based compensation or, as of the end of the last completed fiscal year, there was an outstanding balance of excess incentive-based compensation attributable to a prior restatement.

The required disclosure under Item 402 will include:

- For each restatement, (a) the date on which the issuer was required to prepare the restatement, (b) the aggregate dollar amount of erroneously awarded compensation attributable to the restatement, including an analysis of how the amount was calculated, (c) if the financial reporting measure related to stock price or TSR, the estimates that were used in determining the erroneously awarded compensation attributable to the restatement and an explanation of the methodology used for such estimates, (d) the aggregate dollar amount of erroneously awarded compensation that remains outstanding at the end of the last completed year, and (e) if the amount of erroneously awarded compensation has not yet been determined, that fact and the reasons for such non-determination.

- If recovery would be impracticable, disclosure of the amount of recovery forgone (for each current and former named executive officer individually and for all other executive officers as a group) and a brief description of the reason the issuer decided not to pursue recovery.

- For each current and former named executive officer, the amount of outstanding unrecovered excess compensation that had been outstanding for 180 days or longer since the date the issuer determined the amount owed.

If the issuer was required to prepare a restatement during or after the issuer's last completed fiscal year and concluded that recovery of compensation was not required under the issuer's policy, the issuer must briefly explain why application of the policy resulted in that conclusion.

As long as an issuer provides the new Item 402 disclosure with respect to clawbacks, the issuer need not also make a disclosure under Item 404(a) relating to related party transactions with respect to the clawback activity.

The Item 402 disclosure will need to be provided in XBRL format but will be required only in annual reports on Form 10-K and proxy statements whenever other Item 402 disclosure is required. The disclosure, therefore, will not be required in registration statements under the Securities Act of 1933. In addition, the disclosure will not be deemed incorporated by reference into any filing under the Securities Act of 1933 unless specifically incorporated by reference.

The Summary Compensation Table rules are amended to require that any amounts recovered under a clawback policy reduce the amount reported in the table for the fiscal year in which the original payment was reported and must be identified in a footnote.

Form 10-K Checkboxes

The SEC rule adds two new checkboxes to the cover page of Form 10-K relating to whether the financial statements included in the Form 10-K reflect the correction of an error to previously issued financial statements and whether any of those error corrections are restatements that require a recovery analysis of incentive-based compensation received by executive officers.

Timing of Effectiveness of the Final Rules

Issuers will need to adopt clawback policies no later than December 1, 2023. The clawback policies will need to apply to all incentive-based compensation received by current or former executive officers (after beginning service as an executive officer and who served as an executive officer during the applicable performance period) on or after the effective date of the applicable listing standard. The clawback policy is expected to apply to such compensation even if the compensation is received under a pre-existing contract or arrangement.

Compliance with the new Item 402 disclosure rule is required for all applicable filings with the SEC after the effective date of the exchanges' listing standards, which is October 2, 2023.

Recommended Actions for Listed Manufacturing Companies

- Review any existing clawback policies to determine what revisions are needed to comply with the new rules and listing standards. Among other items, revisions may be needed relating to the individuals covered, the types of compensation covered, the types of restatements that trigger the policy, the lookback period of the policy, the required mandatory nature of clawbacks, and the exceptions to mandated clawbacks. Ensure that the board of directors and/or the appropriate committee of the board, depending on the company’s governance structure, adopts a compliant policy prior to December 1, 2023.

- Review existing incentive-based compensation arrangements and any other plans or agreements that are affected by, or require the payment of, incentive compensation to determine whether there is an existing contractual right to recover compensation, and consider whether to modify the arrangements to permit recovery in the future.

- Consider the impacts on internal controls over financing reporting, quarterly financial reporting closing, and disclosure committee processes; determinations of when a restatement is required; procedures and controls through which clawback policies will be implemented if there is a restatement; and compensation program design. Audit committees and compensation committees will need to work together closely on these items.

2023 Manufacturing Sector M&A: Outlook and Tools to Maximize Strategic Transactions

Outlook

Following the historic highs of 2021, M&A activity in the manufacturing sector and more broadly slowed in 2022 and remains at a cautious but stable pace in 2023.[1] Disclosed industrial

manufacturing deal value and volume for the eight quarters ending December 31, 2022 are presented below.

Challenges include the tightening of debt markets, inflation, volatility in the pricing and availability of raw materials, rising shipping costs and general economic uncertainly[2], although for manufacturers with strong balance sheets the current climate presents opportunities, including to acquire or invest in complementary technology, nearshore certain critical operations or mitigate supply chain risk by acquiring key suppliers, all at valuations that may be at their lowest point in the past few years. Manufacturers looking to divest non-core assets or legacy business lines to provide capital for new initiatives may find willing buyers at the right price, including private equity sponsored platforms which are increasing their roll-up strategy plays in the manufacturing space.

Disclosed Deal Value and Total Volume, Last Eight Quarters

Information cutoff for Q4 2022 is November 15, 2022
Deals included in this graphic are total announced deals (including disclosed and undisclosed).
Source: PwC and Refinitiv

Strategic corporate transactions with emerging technology companies, from minority investments (often termed corporate venture capital or CVC investments) to joint ventures to acquisitions, will continue to enable manufacturers to shortcut or share the significant capital expenditures required to develop technology internally. As early-stage companies face increasing funding challenges, negotiating leverage for larger strategic partners grows.

Structuring Strategic Investments

A key factor in maximizing the use of corporate transactions to gain access to technology is getting the size and structure of the investment right. The approach should be tailored based on the stage of the technology in terms of development, launch, and market acceptance. How radical or aggressive is the solution? How close is it to your current core business? Is it complementary or does it represent an entirely new direction, and if the latter does it fit with your evolving strategy? Consider mechanisms that will help avoid overpaying or overinvesting initially, including performance-based stepped investments in corporate venture capital transactions or contingent post-closing payments (earn-outs) in M&A transactions. If a strategic partnership with another player makes sense, consider the benefits and challenges of a joint venture entity versus a direct contractual partnership, for instance through a joint development agreement.

Corporate Venture Capital

Increasingly utilized by manufacturers exploring technology solutions, a corporate venture capital investment may be the most appropriate path when an early-stage partner needs funding, often to further unproven or pre-revenue technology. The use case may appear to be on the periphery of a strategic investor’s business, but it may have a strategic interest in supporting it, for instance to help develop a new market segment into which your products could ultimately be sold. A corporate venture capital investment can provide access to promising technology without the larger commitment of capital or other resources that a joint venture or add-on acquisition require.

Corporate venture capital does mean minority ownership, which raises issues of control. There is a balance to strike between the desire to exert a measure of control over the strategic direction of what

could turn out to be an important commercial partner or acquisition target on the one hand, and the risk of alienating essential founders or having a cooling effect on the partner's ability to raise capital from other sources or enter into commercial transactions with other parties on the other hand. A seat in the board room together with approval rights over major company actions are typically the focal points of negotiations. If the partner is a potential acquisition target, the strategic partner will want some rights in connection with a potential sale of the company, for instance a right of first offer, right of first refusal or at least notice before the company commits to another buyer. Strategic minority investments are often combined with a commercial agreement to further facilitate the development, manufacturing, or marketing of the technology.

Joint Ventures

Joint ventures may be an appropriate structure to utilize as manufacturers look to partner on newly developed or combined technology. Forming a joint venture allows parties to combine their capital, human, and other resources to advance a potentially profitable project. One player might bring the technology while the other brings credibility, market access, and capital, or the partners may have complementary technology. Entering into a joint venture with an established, well-respected manufacturer may be what an emerging company or a company entering a new geographic market or product segment needs to gain market acceptance. As a precursor to a possible M&A transaction, a joint venture might be attractive to target companies that prefer to maintain autonomy at least for a period of time, and for a potential acquiror it provides an opportunity to test drive the business while deciding whether to acquire it.[3]

Careful consideration should be given to whether a separate joint venture entity is the right fit for the partnership project. Given the time and cost involved in forming and maintaining a separate entity, in many cases entering into a joint development agreement or similar contractual arrangement may make more sense, particularly if the scope of the project is narrow and finite in time. If the project is broader and more complex, is expected to have a significant duration, will require dedicated capital and employees outside of the scope of the parties' current businesses, and/or may be capable of divestiture separate from other segments of the parties' respective businesses, it may make sense to form a joint venture entity to carry the project forward. Liability protection may also factor into the decision. A separate entity may provide a liability shield, although this may be less valuable if the activity overlaps with what the parties are already doing.[4] Finally, customer and supplier relationships and considerations often have an impact on joint venture structuring.

With any joint venture there are issues of control and governance to tackle. Are the parties true equals, or do you have a big fish and a small fish? Such an imbalance may result in majority control for the larger or more established player with minority protections for the other party, essentially a list of things the joint venture entity can't do without both partners on board, such as exit transactions or changes in strategy. Complex dispute resolution and buy/sell provisions are required to enable the joint venture company to navigate through disagreements between the parties on key decisions without paralyzing the business. Put and call options exercisable at agreed-upon points in the future can be utilized to allow one or both parties the opportunity to exit the joint venture if it no longer makes sense for their business.

As in many manufacturing relationships, joint ventures raise competition issues. If there is overlap between what the JV and either of the partners is doing, it can be a challenge to define where the joint venture competes versus the individual partners, geographically and by market segment. The use of exclusive intellectual property licensing provisions with respect to the technology that is the subject of the joint venture should be considered as a way to address the antitrust concerns that

direct contractual competition restrictions might raise. A careful antitrust review is recommended in structuring any joint venture involving competitors.

Divestitures & Acquisitions

A key part of many current strategies in the manufacturing sector is divesting or spinning off non-core or legacy businesses including those centered on older, less profitable and/or increasingly supplanted technology, for instance internal combustion engines in the automotive space, both to streamline operations and provide the capital for growth plays in new or more favored technology. For a divestiture to provide needed capital, it is critical to execute the sale while the business line still has value in the marketplace, which becomes more challenging as the adoption of newer or more favored technology progresses. When considering a divestiture to a private equity sponsor or portfolio company, care should be taken up front to determine with the buyer the nature and length of any transition services or manufacturing agreements the buyer requires to operate the business immediately following the closing.[5]

If a manufacturer is taking the significant step of acquiring a company or key asset, ideally the subject technology has proved out and perhaps even comes with an established or ready-made customer base. The acquiring manufacturer may lack the resources to develop similarly effective technology in house. Due diligence is at a premium in this context, including technical, intellectual property, existing employment and incentive arrangements, environmental (particularly if there is an acquired site with manufacturing operations) and product testing, warranty, and liability matters.

Purchase price structuring plays an important role. The technology and use case may be well-established but the target company's projections may still be rosier than the buyer's more conservative business case, or may be based on the market's adoption of a next generation product. Earn-outs remain a key tool to bridge the valuation gap, with an often-significant portion of the potential total purchase price structured as contingent payments based on the achievement of mutually developed goals for the business, for instance UL certification and launch of a next generation product or the achievement of specified financial metrics such as EBITDA, hardware sales and gross margin or software and related services revenue.

Often acquiring a target company's engineering team is as important as any other asset associated with its business, putting a premium on employee retention. Retention bonuses payable post-closing can be tied not only to remaining employed for a specified period of time but also to the business achieving metrics similar to those used in purchase price earn-out structures. In addition to providing key employees with performance-based incentives, aligning employee retention bonus metrics with seller earn-outs aligns interests among those stakeholders in finalizing negotiations and getting necessary target company approvals for the transaction.

Conclusion

While economic headwinds exist, strategic opportunities abound, and manufacturers with cash on hand or the ability to raise it through tactical divestitures have the ability to make significant strides in evolving their businesses through acquisitions of emerging technology or critical suppliers. Choosing the right structures and mechanics in deal making is paramount if manufacturers hope to maximize the impact of corporate transactions in 2023 and beyond. Consult with internal and external deal professionals early and often as opportunities arise.

[1] Michelle Ritchie, "Industrial Manufacturing: US Deals 2023 outlook," *PwC*, January 2023.

[2] *Id*.

[3] Practical Law Company, "*Joint Ventures: Overview*," 2023.

[4] *Id*.

[5] Brad Hehl, Joern Buss, Abhi Ahuja, Constantin Gall, "How auto suppliers can navigate EV technology disruption in four steps," *EY Parthenon*, December 2021.

The Dawn of Generative AI in Manufacturing: Opportunities, Implications, and the Future

Introduction

The history of human progress has been characterized by transformational discoveries that have opened the doors to a surge of societal and technological change. The Agricultural Revolution, the Industrial Revolution, and the advent of the Internet have each changed the way we live, work, and interact with the world. Now, we stand on the edge of another major shift: the era of generative AI. This new era is not just about automating tasks but about AI systems that can independently create and generate new ideas, designs, and solutions.

Similar to the steam engine that drove the factories of the 19th century and the Internet revolution that connected billions of people in the 20th, generative AI is poised to redefine the 21st-century manufacturing industry. By using the power of large language models (LLM) and advanced machine learning algorithms, generative AI can quickly generate new ideas, designs, and solutions that often go beyond human capability, offering new opportunities while also posing new challenges.

Opportunities and Positive Effects

Generative AI holds the potential to revolutionize the manufacturing industry. One of the most significant opportunities lies in the realm of design. Generative AI design tools can create potential product designs by exploring all possible permutations and combinations within a given set of constraints. For example, when designing an airplane, designers often have to brainstorm and test hundreds of designs. Designers can use AI to iterate through hundreds of designs in a much shorter time to find the optimal balance of strength, weight, aerodynamics, and cost by asking the AI to find the optimal combination for their needs, as well as to suggest modifications in real-time according to the designer's requests. This could dramatically accelerate the design process, reduce costs, and potentially result in more efficient and innovative products.

In addition, generative AI could revolutionize supply chain management. By learning from vast amounts of data, generative AI models can predict supply and demand trends, optimize inventory management, and even propose new business strategies. A supply manager could use generative AI to constantly monitor inventory and autonomously order new materials when supply levels run low, perhaps using new suppliers or supply routes based on logistical constraints. At the same time, AI could monitor consumption habits to make new connections in consumer behavior much faster than a team of human analysts and provide recommendations for new products aligned with consumers preferences. This could lead to significantly improved operational efficiency and profitability.

Further, generative AI may play a key role in quality control. Advanced generative AI algorithms can detect anomalies and predict failures in manufacturing processes and provide reasons for such

failures, enabling companies to proactively address issues before they escalate. This could significantly reduce downtime, improve product quality, and enhance customer satisfaction.

Key Legal and Business Risks Manufacturers May Face When Adopting AI

While use of generative AI may offer substantial new opportunities and positive effects, it also brings a set of challenges with both legal implications as well as more general business risk for manufacturers to understand and manage as they integrate generate AI into their operations.

As a starting point, companies need to have a clear understanding of who owns the data used to train the generative AI models. Even if the training data is made available by publicly accessible Internet sources, it may still be subject to copyright protections on behalf of the authors of the training data. Similarly, in the context of AI tools that automatically generate software code, the training data may be subject to open source licensing obligations (and it may be difficult for companies to verify whether this is the case), which can result in manufacturers being obligated to make available any source code that includes portions covered by the open source obligations. Some models may also be susceptible to generating outputs that are similar or identical to the training data, which may break trade secret or other applicable protections on confidential information. These issues can be exacerbated where companies use confidential information (either their own or that of third party) to fine-tune the generative AI models and/or as inputs to the generative AI models. Given such considerations, manufacturers should clearly identify who owns the data their models use, and to the extent there are ownership risks, find alternative ways to train on similar data or negotiate directly for authorization to use the data.

Another potential downside is the risk of amplifying existing biases. If the data used to train generative AI algorithms contains biases, the generative AI model's decisions and recommendations have the potential to perpetuate and potentially amplify these biases. For example, the available training data for a given manufacturing process may be unequally distributed amongst the possible events that could occur during the process, such that the resulting model may be biased towards detecting or recommending certain events or actions over others. In addition, biases in algorithms used for employee management processes could lead to unfair outcomes in areas such as hiring, promotions, and performance evaluations, which could expose companies to liability from such outcomes. Similarly, where manufacturers sell consumer products for certain demographic groups, they may need to validate against biases that may be introduced by generative AI models in the design process. It will be important to maintain transparency regarding how the generative AI makes decisions, which is key to understanding its biases.

Moreover, the increasing reliance on generative AI could pose new security risks. As manufacturing processes become more digitized and interconnected, they could become more vulnerable to cyber-attacks. While generative AI has the potential to greatly improve manufacturing processes and supply chains, it also can be manipulated, hacked for trade secrets or shut down by cyber-attacks. This could potentially disrupt manufacturing operations and compromise sensitive data. In addition, as companies move more operations from human oversight to computer automation, it will be necessary to ensure effective security policies are in place and executed to mitigate increased security risks.

Another concern resulting from the overreliance of generative AI is the "sameness" that AI brings. Even where generative AI models are intentionally designed to generate outputs that vary from the examples used in training, they may lack the capability of spontaneous idea creation that is a hallmark of human creativity. Thus, the potential exists of a world where designs of products are rehashes of previous designs despite their unique appearance. On the other hand, when designed to

have greater freedom to generate new content, generative AI models are susceptible to “hallucinating”—generating content that has little or no factual basis. Therefore, it is important to not over-rely on AI and to maintain a fair balance of AI-generated ideas and human creativity while designing. Designers should use AI to make work more efficient, not to do their jobs for them. Companies should work to establish human oversight over outputs from models to mitigate issues from hallucinations, particularly where outputs such as product designs or manufacturing process controls may lead to product liability concerns if the model’s outputs are not properly validated.

Last, the adoption of generative AI could exacerbate existing digital divides. Companies that can afford to invest in capital-intensive aspects of implementing AI technology, such as deploying the hardware resources required to operate complex machine learning models, may gain a significant competitive advantage, potentially widening the gap between large corporations and smaller businesses.

Conclusion

The advent of generative AI marks a new era in the manufacturing industry. As this new era arrives, one thing is certain: like the Agricultural Revolution, the Industrial Revolution and the Internet Era, the AI era will bring mass changes to society and technology. As with any transformational event, there will be challenges and obstacles, but with foresight and careful planning, we can navigate these changes and harness the power of generative AI to usher in a new era of innovation and prosperity in the manufacturing industry.

The potential of generative AI to improve design, quality control, and optimize supply chain management is tremendous. However, it also brings with it a set of challenges and potential downsides that must be carefully managed.

To navigate this new landscape, it will be necessary to approach it with a sense of balance. We must harness the power of AI while also ensuring that its adoption does not exacerbate social inequalities, perpetuate biases, or compromise security. Companies will need to look hard at how they can apply generative AI without decimating the workforce or abdicating decision-making to it. With thoughtful application and responsible use, generative AI can truly become a key arm of manufacturing, moving us into a new era of innovation. The AI era opportunities are vast and its potential to transform manufacturing is immense with profound implications.

Generative AI is more than just a new tool for manufacturing; it’s a transformative force that, like the industrial revolutions before it, has the potential to reshape the industry and society in ways we are only beginning to understand. The dawn of generative AI promises an era where creativity is not limited to human minds but can be mechanized, scaled, and optimized. Yet, it is up to policymakers, business leaders, workers, and society as a whole to chart the course for this new technology, shaping its use to ensure a future that is not only more efficient and prosperous, but also more just. As we embark on this journey, we must remember that our goal is not merely to create a more advanced industry, but a more equitable, sustainable, and prosperous future.

Authors- Alexander Misakian Frank S. Murray Jr Andrew J. Salomone Roberto J. Fernandez Scott D. Anderson Marcus W. Sprow Erik K. Swanholt Nicholas R. Johnson Kristin McGaver Sikora Nathan A. Beaver Trent M. Johnson Tim Patterson Amanda K. Beggs Dorothy E. Watson Samuel J. Winer Joshua A. Agen Jessica S. Lochmann Leigh C. Riley John K. Wilson Jonathan H. Gabriel Steven H. Hilfinger John D. Lanza Shabbi S. Khan Nikhil T. Pradhan Michelle Y. Ku Chase J. Brill

National Law Review, Volume XIII, Number 192