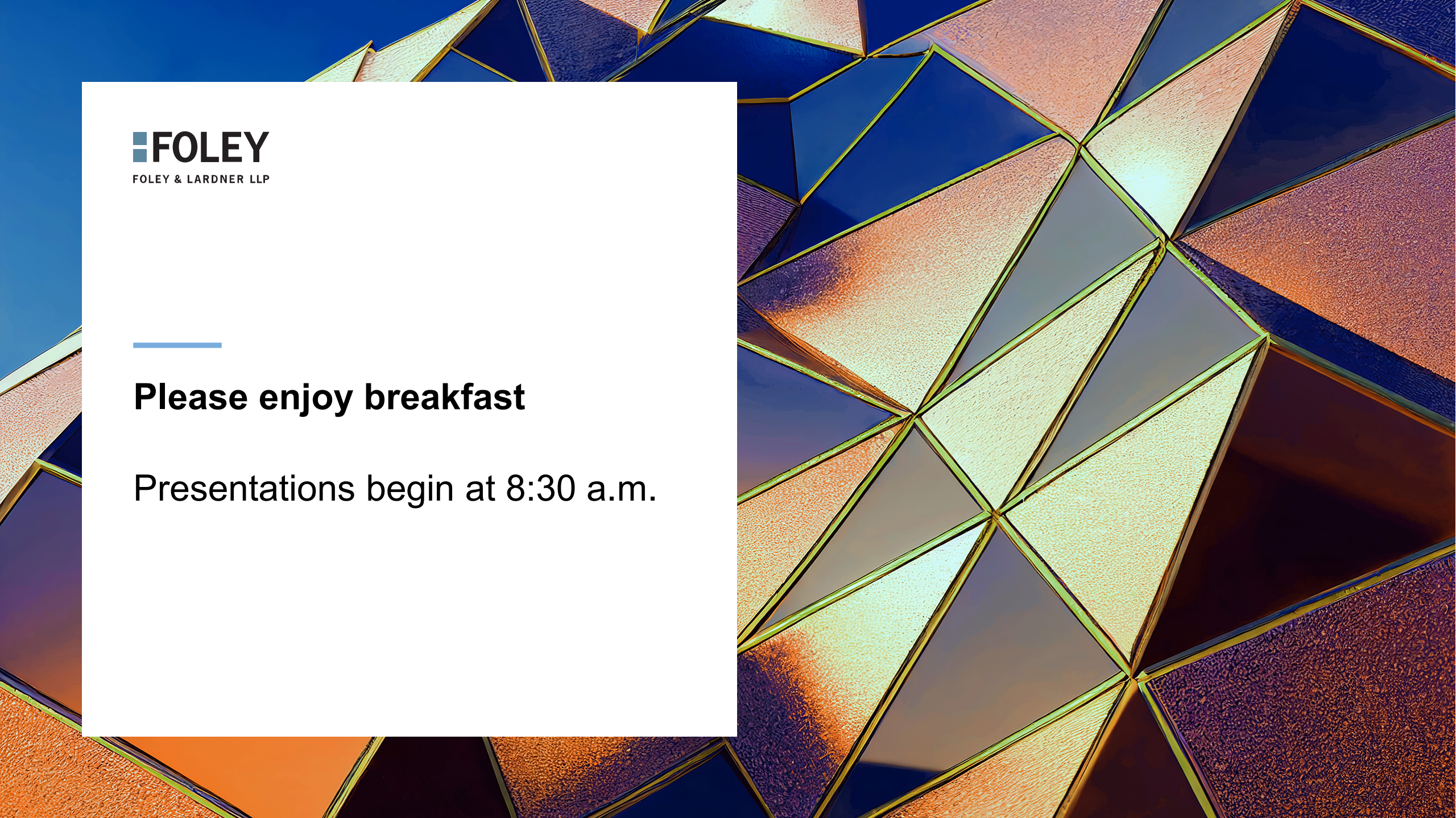
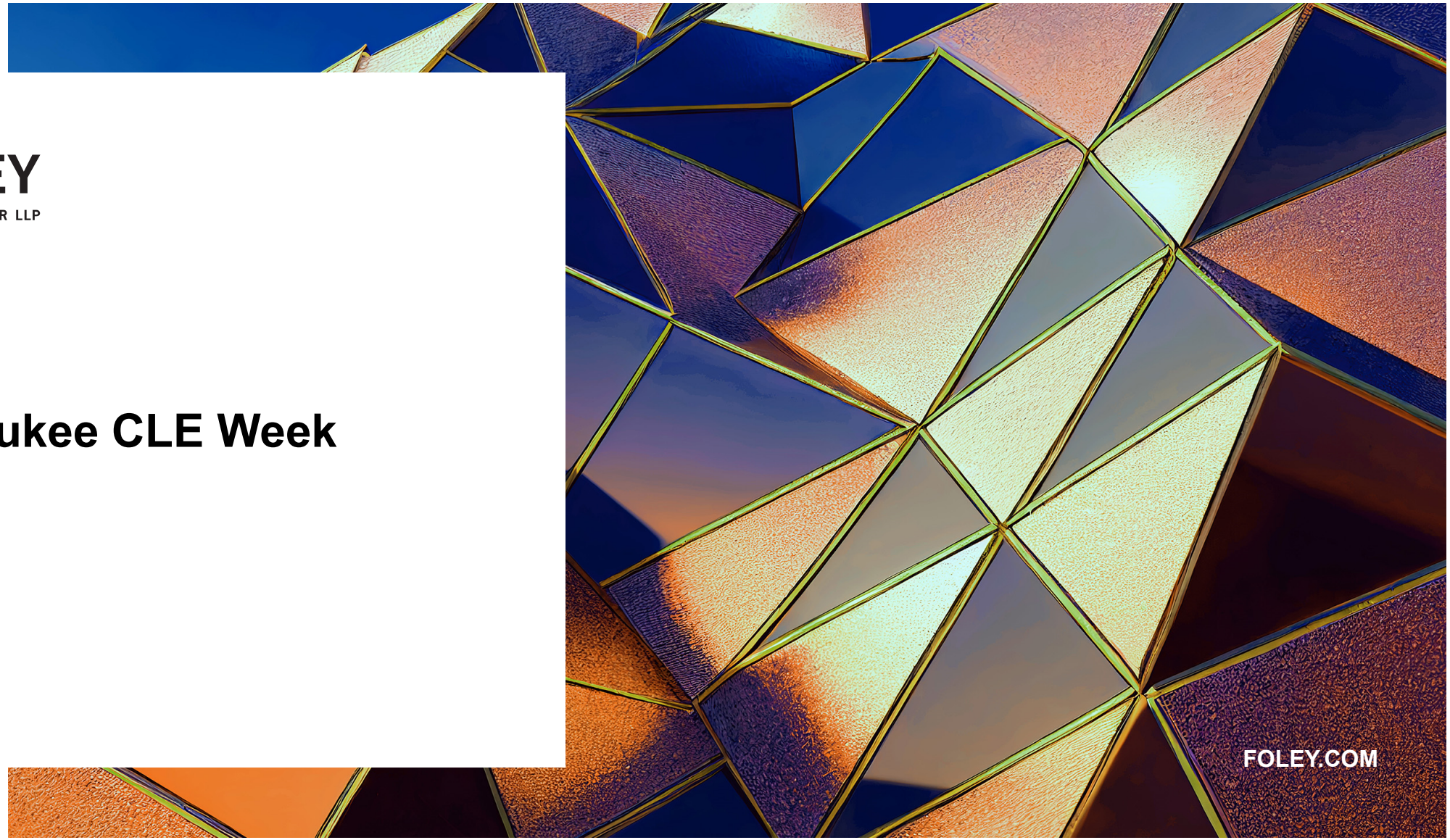

FOLEY
FOLEY & LARDNER LLP
Please enjoy breakfast
Presentations begin at 8:30 a.m.

FOLEY

FOLEY & LARDNER LLP

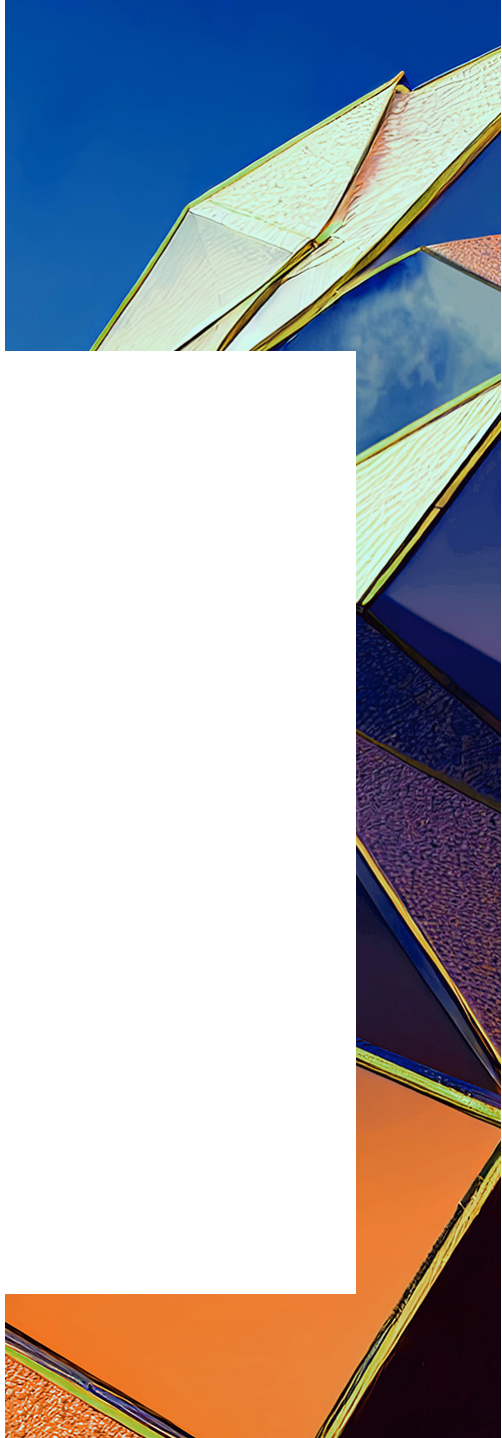
Milwaukee CLE Week

December 7, 2023



Housekeeping

- Please help yourself to breakfast
- Wi-Fi information can be found at your desk
- Presentation materials can be downloaded from www.foley.com/milwaukeecleweek2023
- Complete CLE form and survey for sessions attended
  - Leave with registration team before departure



FOLEY

FOLEY & LARDNER LLP

Top Antitrust Issues in 2023, and What You Need to Know in the Year Ahead

December 6, 2023

Presenters

Elizabeth A. N. Haas
Partner | Milwaukee

T: 414.297.5083
E: ehaas@foley.com

Kate Gehl
Senior Counsel | Milwaukee

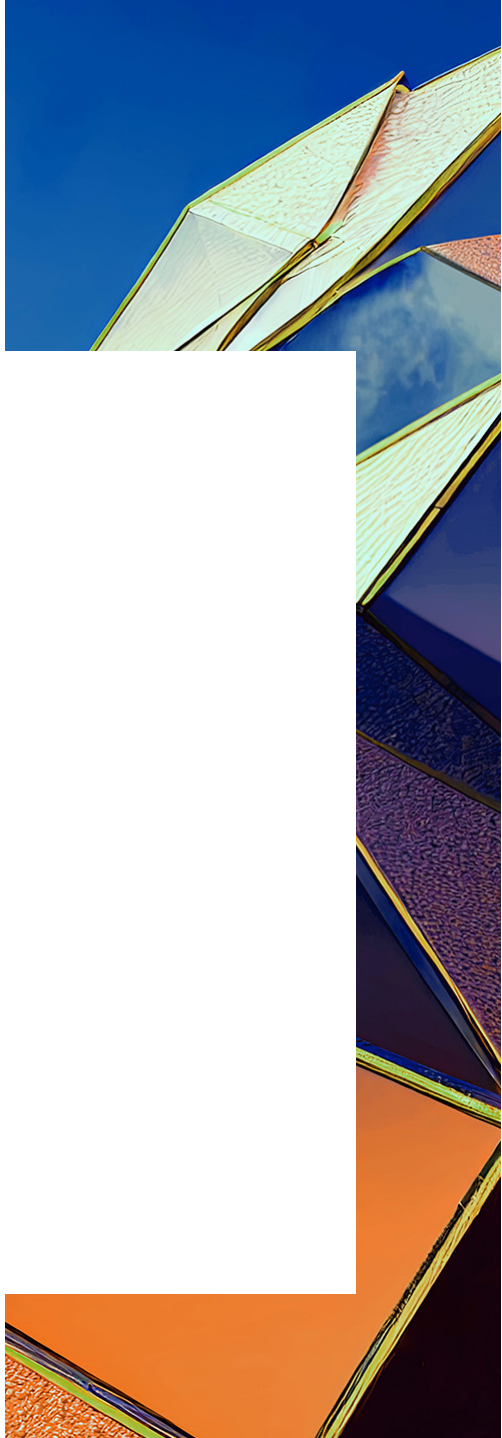
T: 414.297.5279
E: kgehl@foley.com

Ian Hampton
Senior Counsel | Milwaukee

T: 414.297.4912
E: ihampton@foley.com

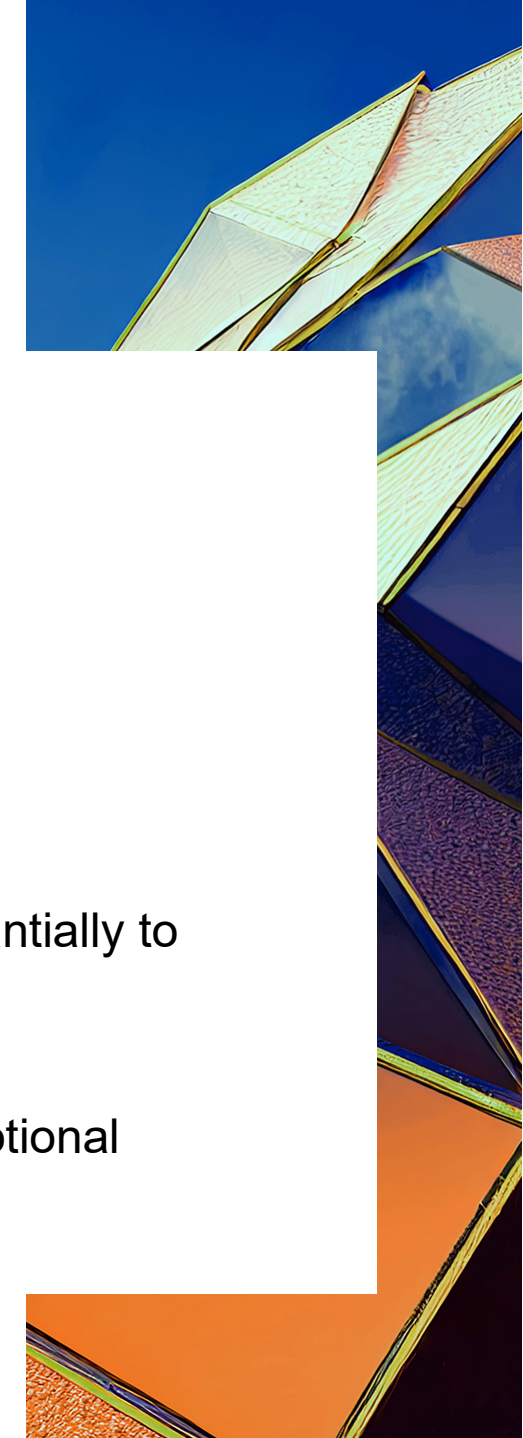
Agenda

- Antitrust Overview
- Today's Antitrust Enforcement Environment
- Antitrust Hot Topics & What Lies Ahead
  - Draft Revised Merger Guidelines & Proposed Hart-Scott-Rodino Process Reforms
  - Interlocking Directorates
  - Renewed Enforcement of the Robinson-Patman Act
  - Antitrust in Labor Markets
  - DOJ's Withdrawal from Policy Statements on Information Sharing
  - Expansion of Power Under Section 5 of the FTC Act
  - Application of Antitrust to Artificial Intelligence
- Best Practices for Reducing Antitrust Risk



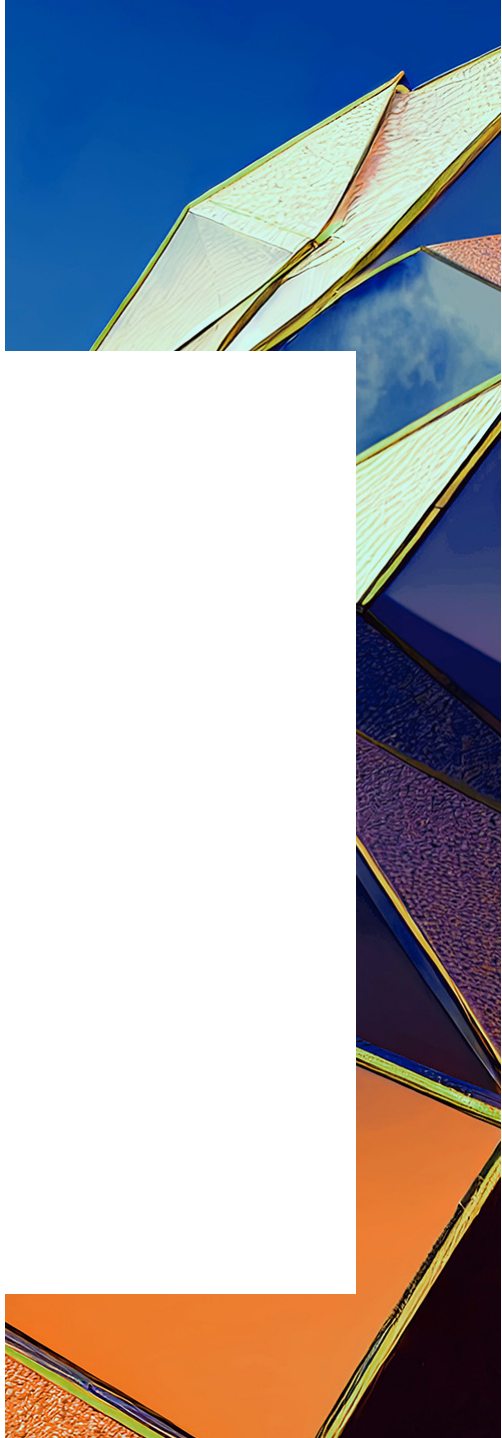
U.S. Antitrust Law Overview

- Section 1 of Sherman Act
  - Prohibits agreements that unreasonably restrain trade
- Section 2 of the Sherman Act
  - Prohibits monopolies, attempts to monopolize, and conspiracies to monopolize
- Section 5 of the FTC Act
  - Prohibits “unfair” methods of competition
- Section 7 of the Clayton Act
  - Prohibits mergers or acquisitions where “the effect of such acquisition may be substantially to lessen competition, or to tend to create a monopoly”
- Robinson-Patman Act
  - Prohibits price discrimination and discrimination in the payment or provision of promotional services
- State antitrust laws



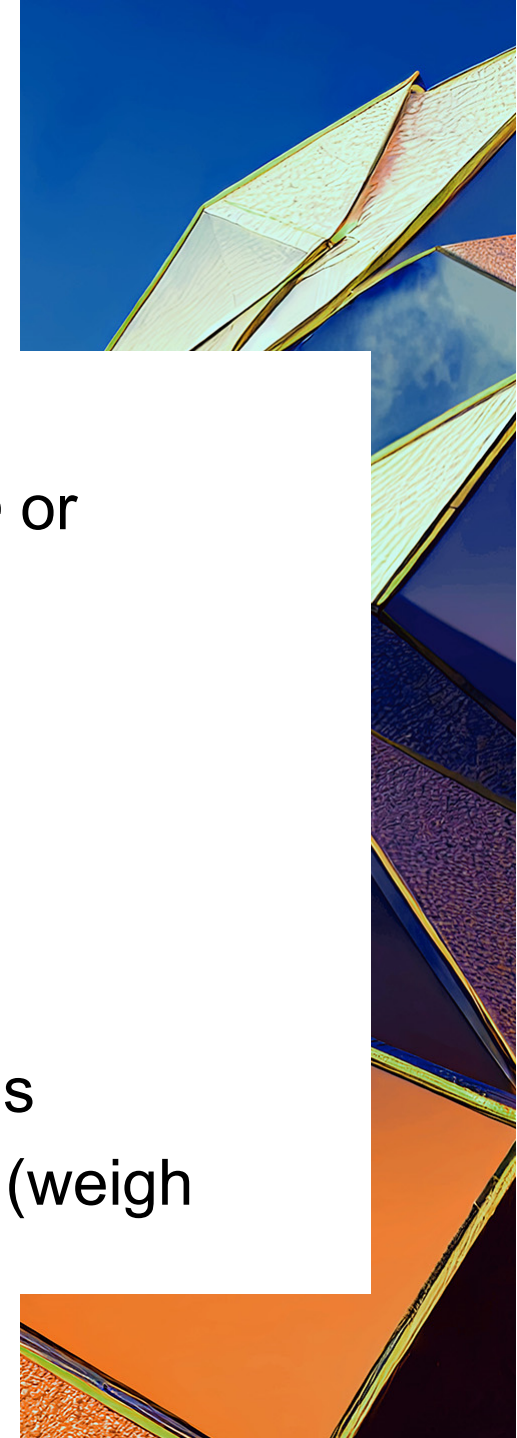
U.S. Antitrust Law Overview

- Criminal and civil enforcement actions from DOJ Antitrust Division
- Civil enforcement actions from the Federal Trade Commission
- State Attorneys General enforcement actions
- Private party litigation
- Fines, penalties, and treble damages
- Attorneys' fees
- Reputational harm
- Time, burden, and expense to litigate is significant

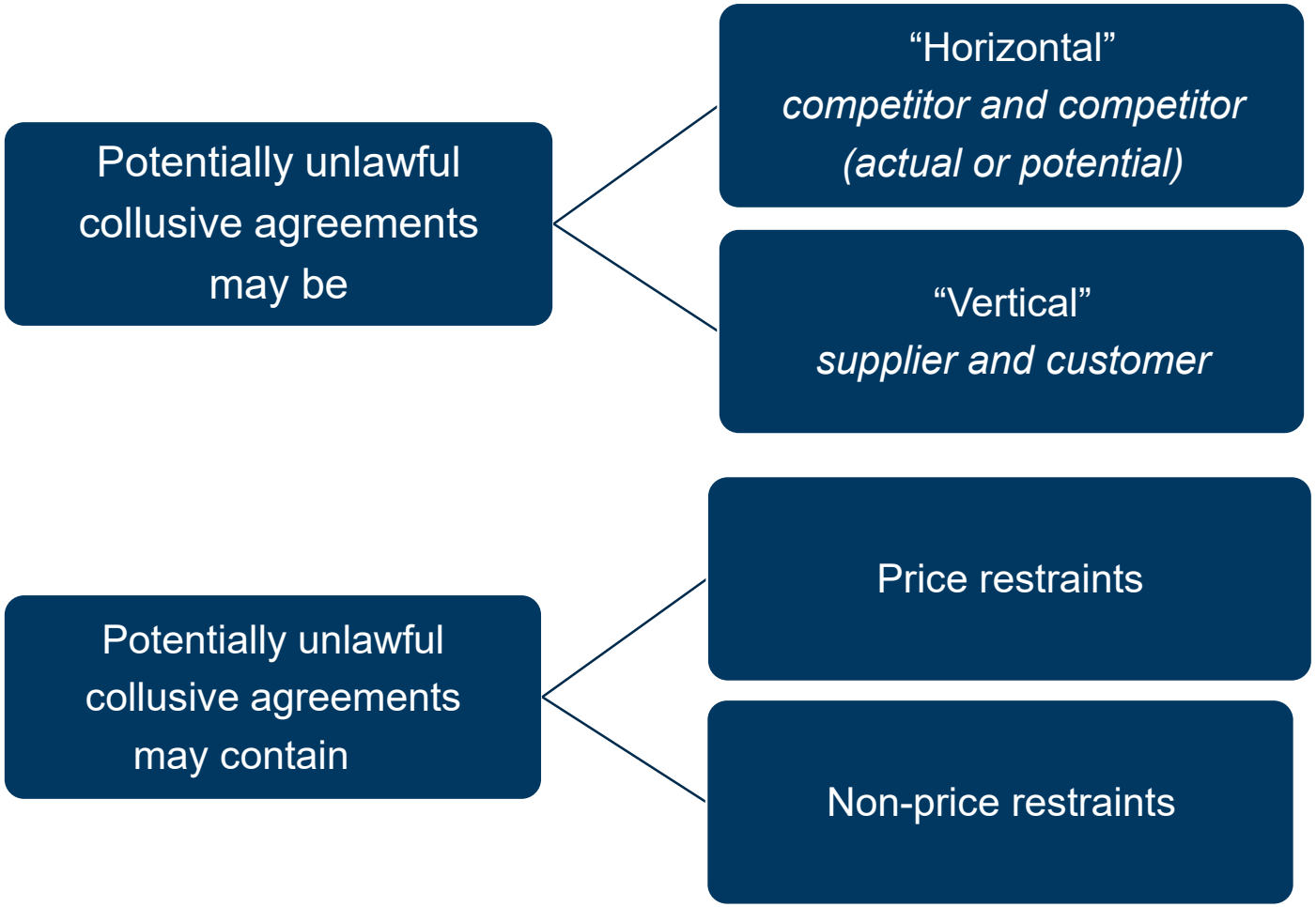


The Sherman Act – Section 1 (Agreements)

- Prohibits agreements that unreasonably restrain trade
- Certain conduct viewed as “naked” restraint of trade that is *per se* or automatically unlawful
- *Per se* violations include agreements with competitors to:
  - Fix prices
  - Rig bids
  - Allocate products / services / territories / customers
  - Fix wages or refrain from hiring each other’s employees
- Unsuccessful conspiracies can still be considered *per se* violations
- Other types of agreements are analyzed under the rule of reason (weigh procompetitive benefits with anticompetitive effects)



Sherman Act – Section 1

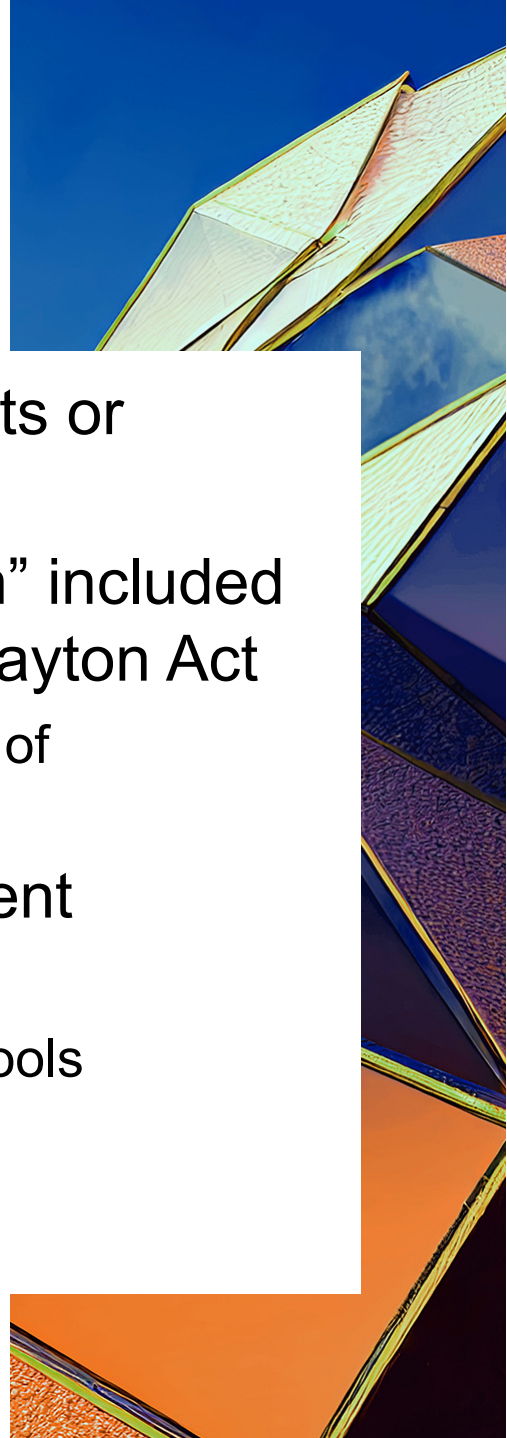


The Sherman Act – Section 2 (Unilateral Conduct)

- Monopolization or Attempt to Monopolize
  - Monopolization
    - Possession of monopoly power in a relevant antitrust market
    - Acquired or maintained that monopoly position through **anticompetitive or predatory means** (i.e., not by superior business acumen, historical accident, or luck)
  - Attempt to Monopolize
    - Specific anticompetitive intent
    - Predatory or exclusionary act
    - Dangerous probability of success (i.e., that defendant may gain a monopoly)

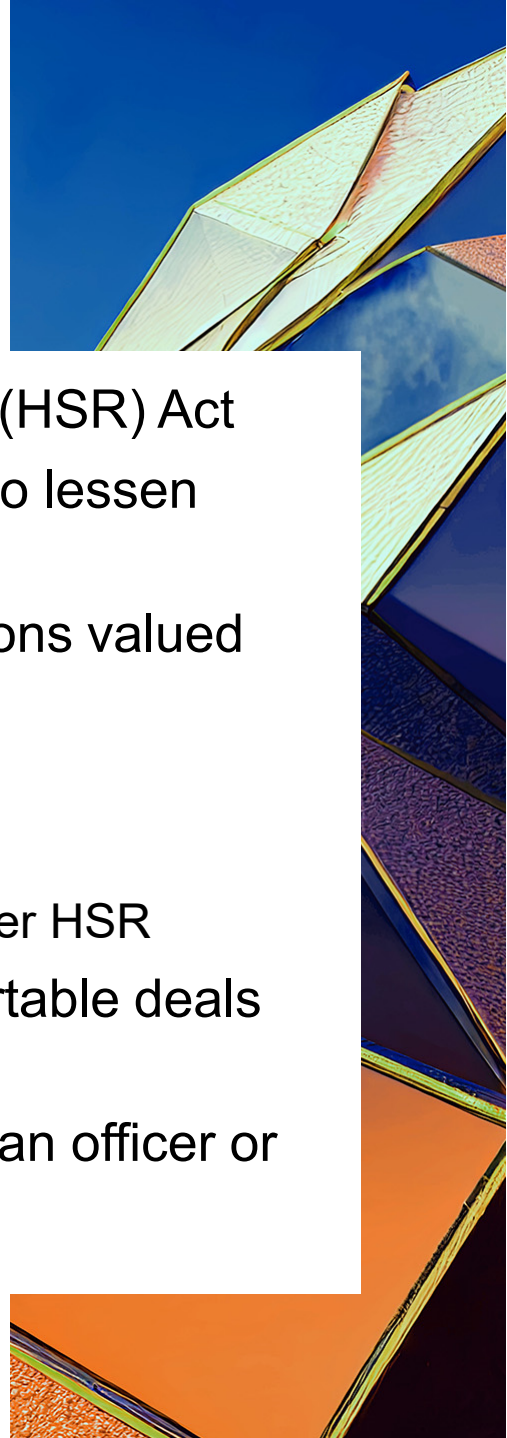
Section 5 of the FTC Act

- Prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce
- Historically, as a matter of practice, “unfair methods of competition” included any conduct that would violate the Sherman Antitrust Act or the Clayton Act
  - The FTC’s interpretation of Section 5 and what constitutes an “unfair method of competition” has recently expanded beyond these historic boundaries
- Under the FTC Act, the FTC has both investigatory and enforcement authority
  - FTC uses subpoenas or civil investigative demands (CIDs) as investigatory tools
  - FTC enforces Section 5 by:
    - Bringing actions for injunctive relief in federal court; or
    - Using its administrative process and adjudicative proceedings



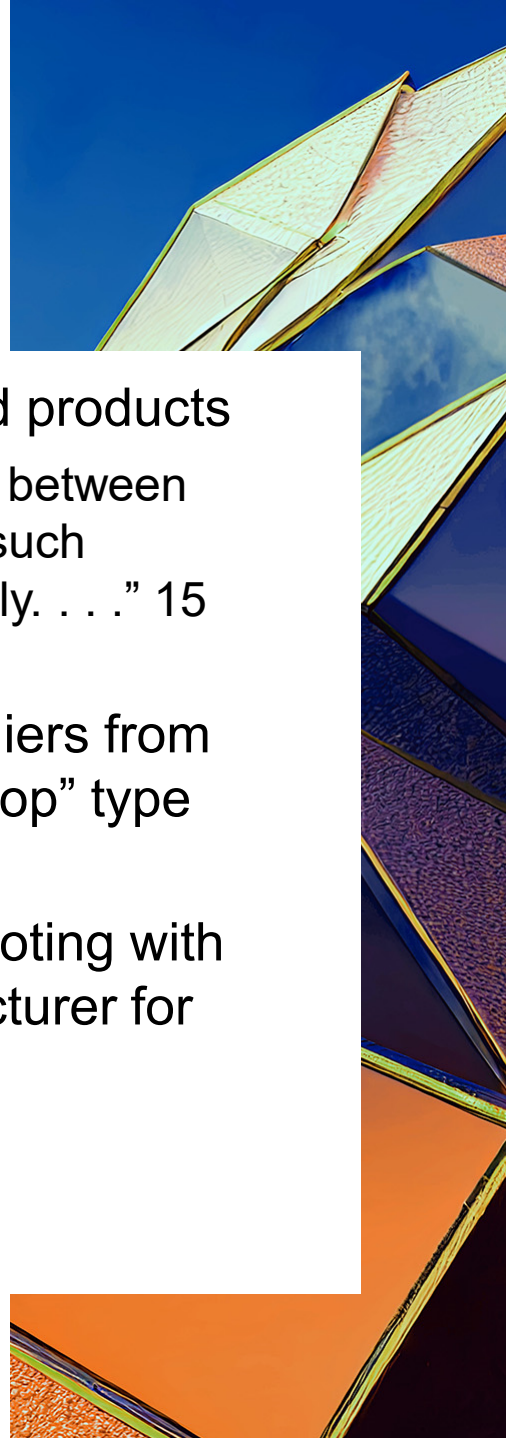
The Clayton Act and Hart-Scott-Rodino Act

- FTC and DOJ review mergers through the Clayton Act and Hart-Scott-Rodino (HSR) Act
- Section 7 of the Clayton Act prohibits mergers or acquisitions that “may” tend to lessen competition or create a monopoly
- HSR requires 30-day waiting period (extendable by DOJ/FTC) for all transactions valued above $111.4 million
  - Threshold changes every year based on inflation
  - Valuation rules are complicated – consult counsel whenever close
  - Joint ventures, formation of new entities, acquisition of greater interests all may trigger HSR
- Note that enforcers have broad powers to investigate and challenge non-reportable deals or consummated deals
- Section 8 of the Clayton Act prohibits interlocking directorates, i.e., serving as an officer or director of two competing corporations



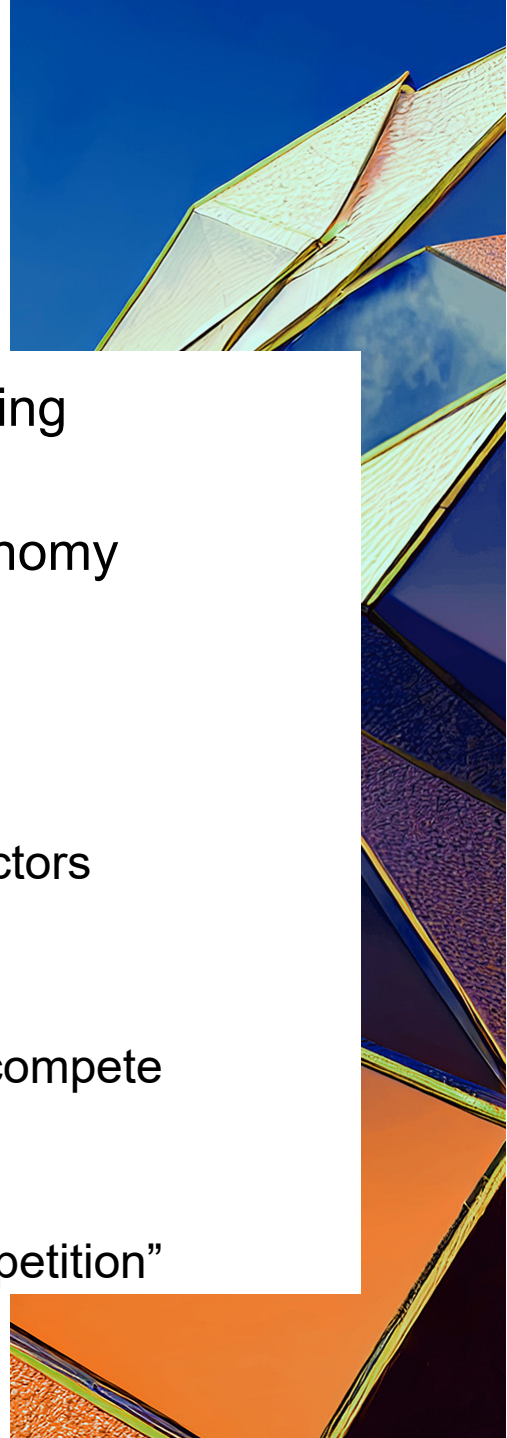
Robinson-Patman Act

- 1936 law designed to address price discrimination in the sale of like goods and products
  - "It shall be unlawful for any person engaged in commerce . . . to discriminate in price between different purchasers of commodities of like grade and quality . . . where the effect of such discrimination may be substantially to lessen competition or tend to create a monopoly. . . ." 15 U.S.C. § 13(a)
- A product of the Great Depression, Congress passed the RPA to prohibit suppliers from giving large scale purchasers more favorable pricing compared to "mom and pop" type stores
- Resellers operating on the same functional level stand on equal competitive footing with regard to pricing and promotional support they receive from the same manufacturer for the resale of the same products
- "Prices" includes more than sticker price
- Rebates, loyalty programs, and volume discounts are within the scope of RPA

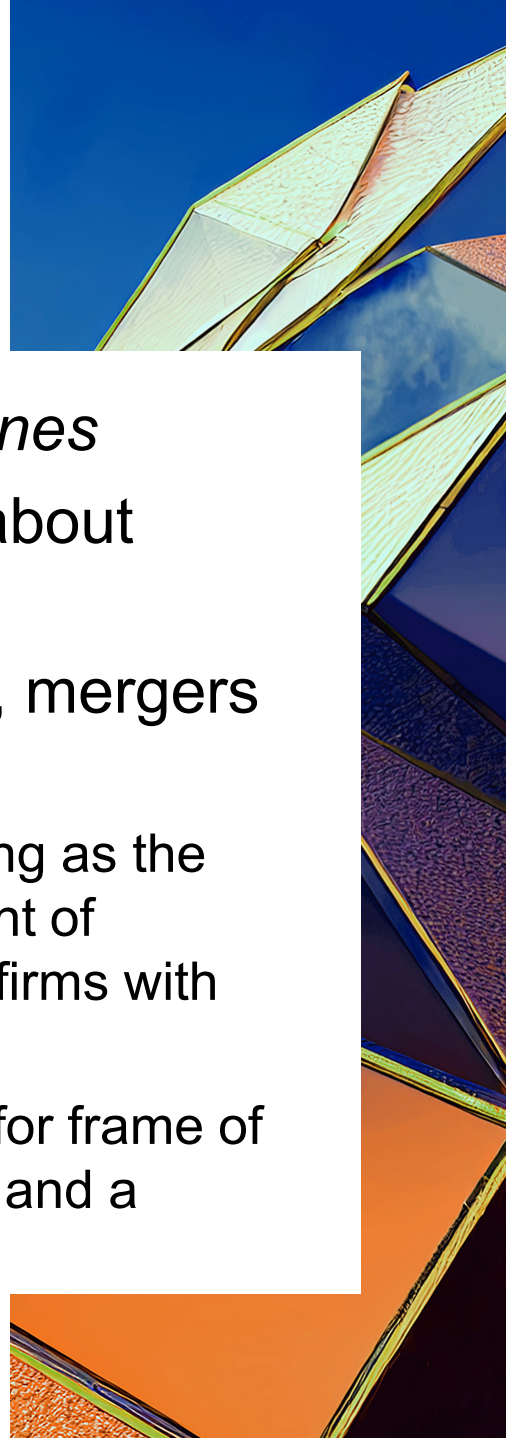


What is Behind the Current Antitrust Enforcement Environment?

- On July 9, 2021, President Biden signed Executive Order 14036, titled “Promoting Competition in the American Economy”
- Adopted a “whole-of-government effort” to promote competition in the U.S. economy
  - Aimed at protecting consumers, workers, and small businesses
- Called for the DOJ and FTC to “enforce the antitrust laws vigorously”
- It includes 72 initiatives by more than a dozen federal agencies including:
  - Increasing scrutiny of mergers, especially in the hospital, banking, and technology sectors
  - Revisiting the Horizontal and Vertical Merger Guidelines
  - Reaffirming the government’s authority to challenge consummated mergers;
  - The FTC is “encouraged to consider” regulations curtailing the use of employee non-compete agreements
  - Reporting on whether food industry practices violate the RPA and FTC Act
  - Making and enforcing rules against airline fees that constitute “unfair methods of competition”

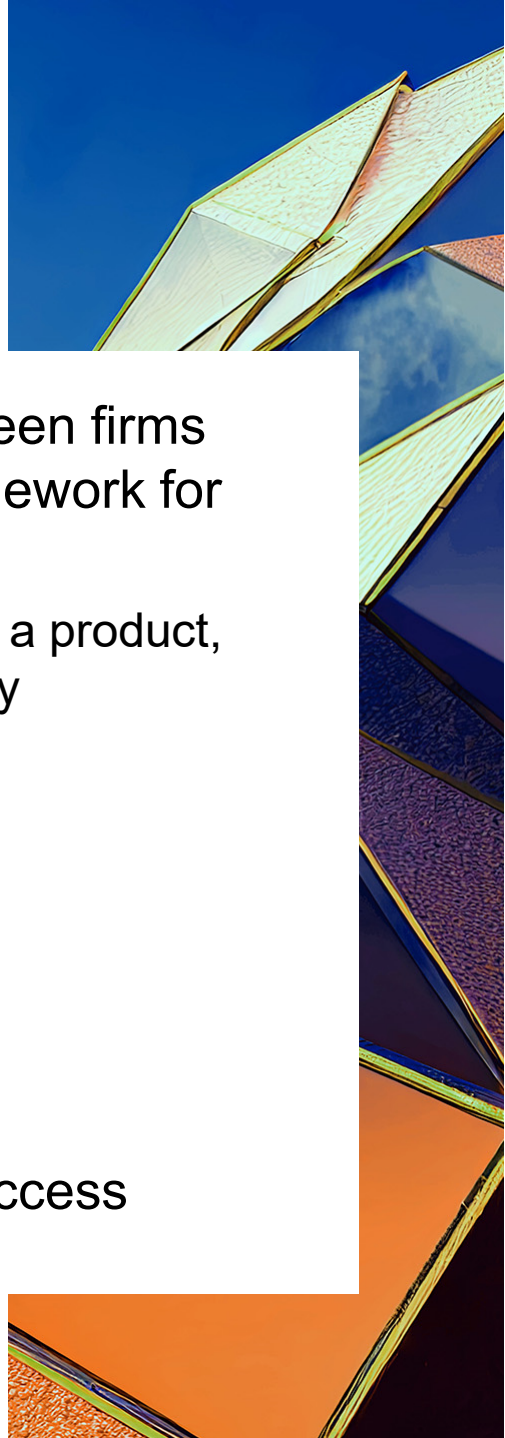


2023 – Year in Review: New Merger Guidelines



- **July 2023**: DOJ/FTC release a draft set of revised *Merger Guidelines*
  - The revised guidelines include broad "structural presumptions" about when mergers violate the antitrust laws
- The new *Merger Guidelines* presume that horizontal mergers (i.e., mergers between competitors) are illegal if, among other things:
  - The horizontal merger results in a firm with a market share above 30%, so long as the merger creates a change in Herfindahl-Hirschman Index (HHI, a measurement of market concentration) of at least 100 (which would be met by combining two firms with market shares of 29% and 2%, respectively)
  - The horizontal merger results in an overall market with an HHI above 1,800 (for frame of reference, a market with five equally sized competitors has an HHI of 2,000), and a change in HHI of at least 100

2023 – Year in Review: New Merger Guidelines

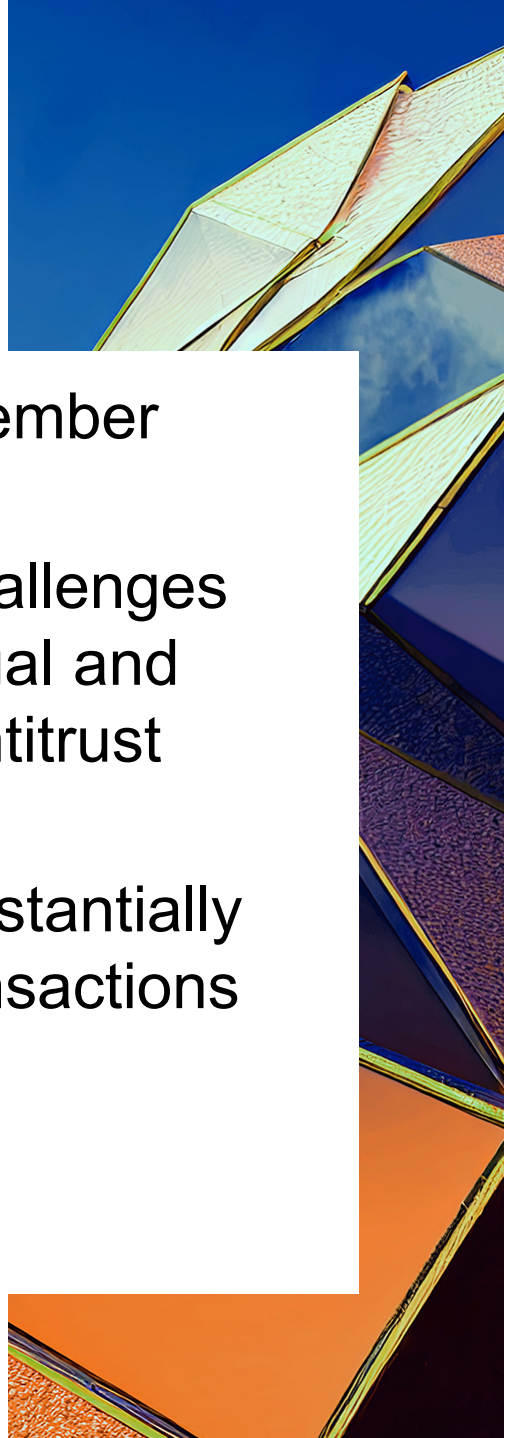


- The new *Merger Guidelines* also warn that vertical mergers (i.e., mergers between firms at different market levels) may act as "a clog on competition" and set out a framework for evaluating their legality:
  - If the merged firm controls more than 50% of the market for the "related product" (i.e., a product, service or customer that rivals need to compete) indicates that the vertical merger may substantially lessen competition, subject to rebuttal evidence.
  - Below that level, agencies will consider "plus factors," including but not limited to:
    - Trend toward further vertical integration
    - Nature and purpose of the merger
    - The relevant market is already concentrated
    - The merger increases barriers to entry
- In 2023, DOJ and FTC have challenged a variety of transactions with mixed success

2023 – Year in Review: HSR Process Reforms

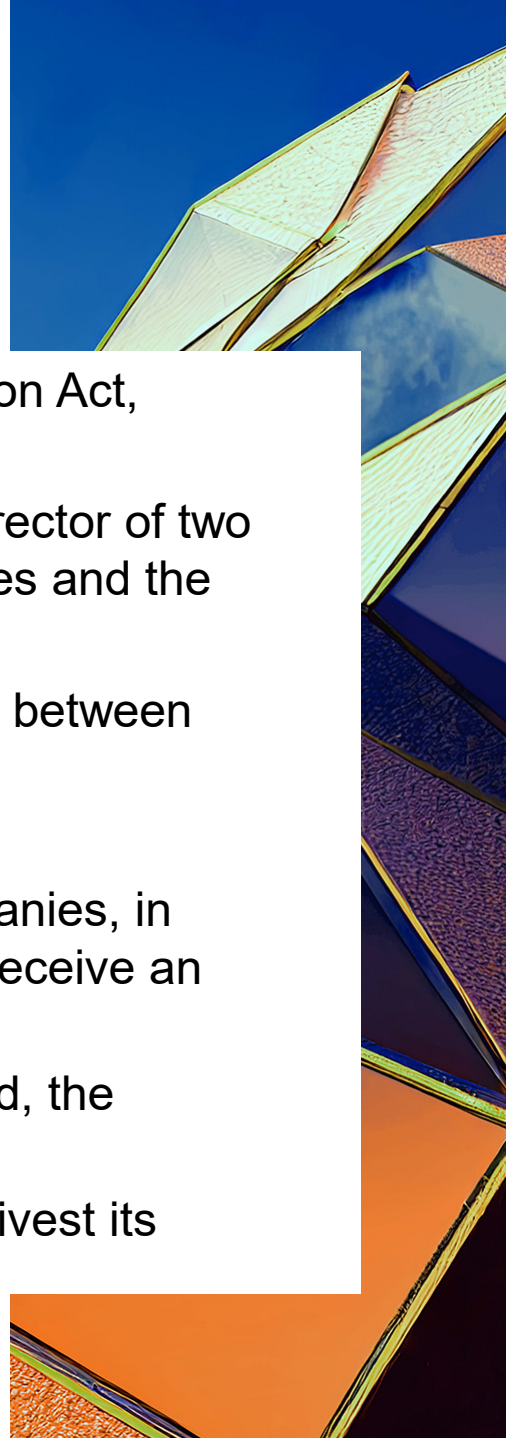
- **June 2023**: FTC and DOJ propose changes to HSR pre-merger notification and report form
- Changes that may increase filing burdens include but are not limited to:
  - Detailed narrative explaining any current or planned area of competition between the merging parties
  - Detailed narrative explaining any supply relationship between the merging parties
  - The narrative about the rationale for the transaction with cross-references to relevant deal documents
  - Expanded scope of document-search obligations to include documents prepared by "supervisory deal team leads" (even if not officers or directors) and "draft" documents
  - Significantly expanded requirements to list prior acquisitions in overlapping lines of business

2024 – Outlook:
New Merger Guidelines and HSR Reforms



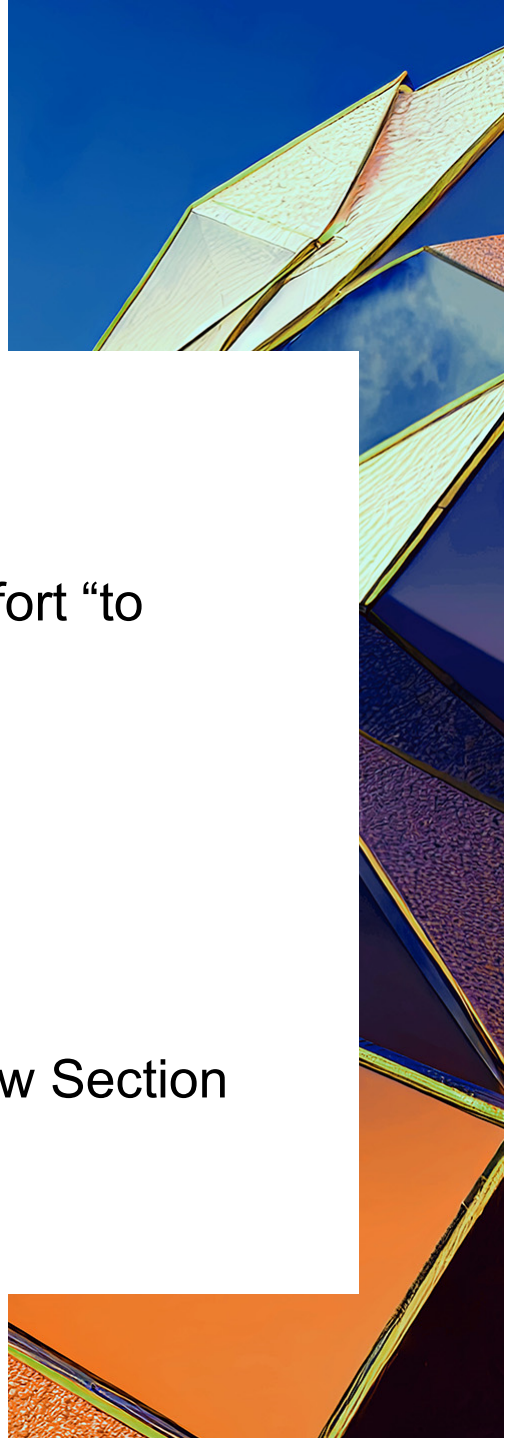
- Public comment period for new *Merger Guidelines* closed in September 2023, and the agencies will likely finalize their guidance shortly
- Unless the guidelines are substantially changed, expect to see challenges to horizontal and vertical mergers the guidelines presume are illegal and litigation over whether those presumptions square with existing antitrust law
- Once finalized, the proposed HSR process changes will likely substantially increase the information required in filings for HSR-reportable transactions (i.e., that meet $111.4M size-of-transaction test)

2023 – Year in Review: Interlocking Directorates



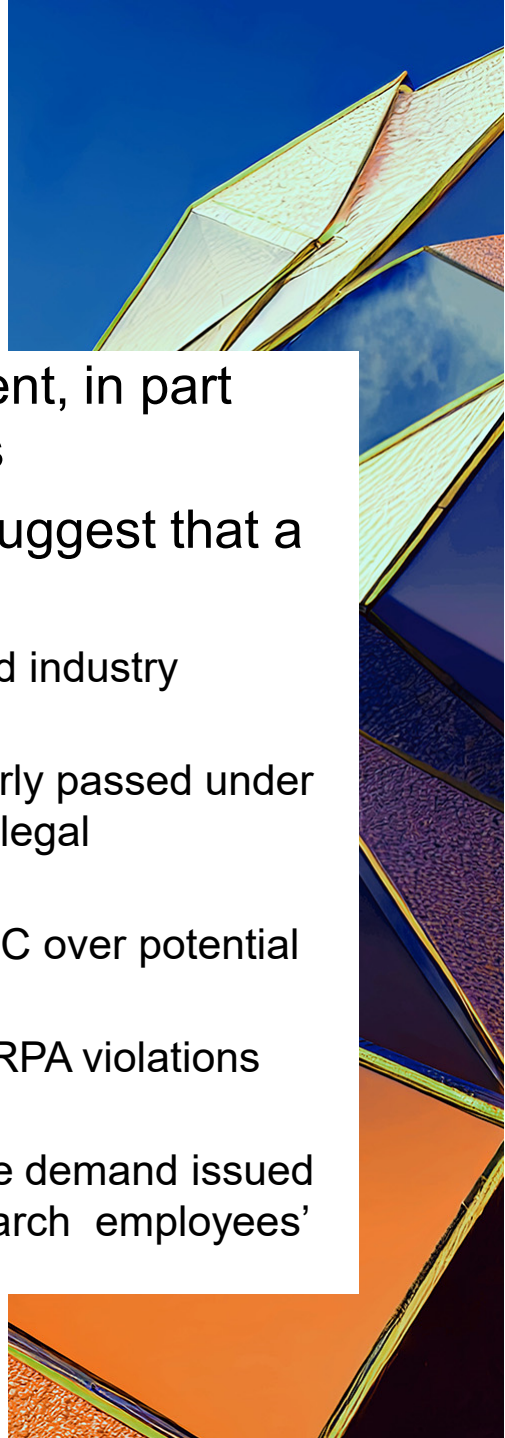
- For the first time in 40 years, the FTC has taken action to enforce Section 8 of the Clayton Act, which prohibits so-called interlocking directorates
- Section 8 of the Clayton Act broadly prohibits individuals from serving as an officer or director of two competing corporations, subject to certain exceptions based on the corporations' finances and the amount of business for which they compete
- **August 2023:** FTC approved a consent order effectively undoing a cash-and-stock deal between private equity firm (Quantum) and natural gas producer (EQT)
  - Quantum and EQT allegedly competed in natural gas market
  - Under the proposed deal, EQT would have acquired two of Quantum's portfolio companies, in exchange for which Quantum would become one of EQT's largest shareholders and receive an EQT board seat
  - FTC complaint alleged that by agreeing to install a Quantum designee on EQT's board, the parties created an interlocking directorate in violation of Section 8
  - Consent order prohibits Quantum from occupying EQT board seat and requires it to divest its EQT shares, among other remedies

2024 Outlook: Interlocking Directorates



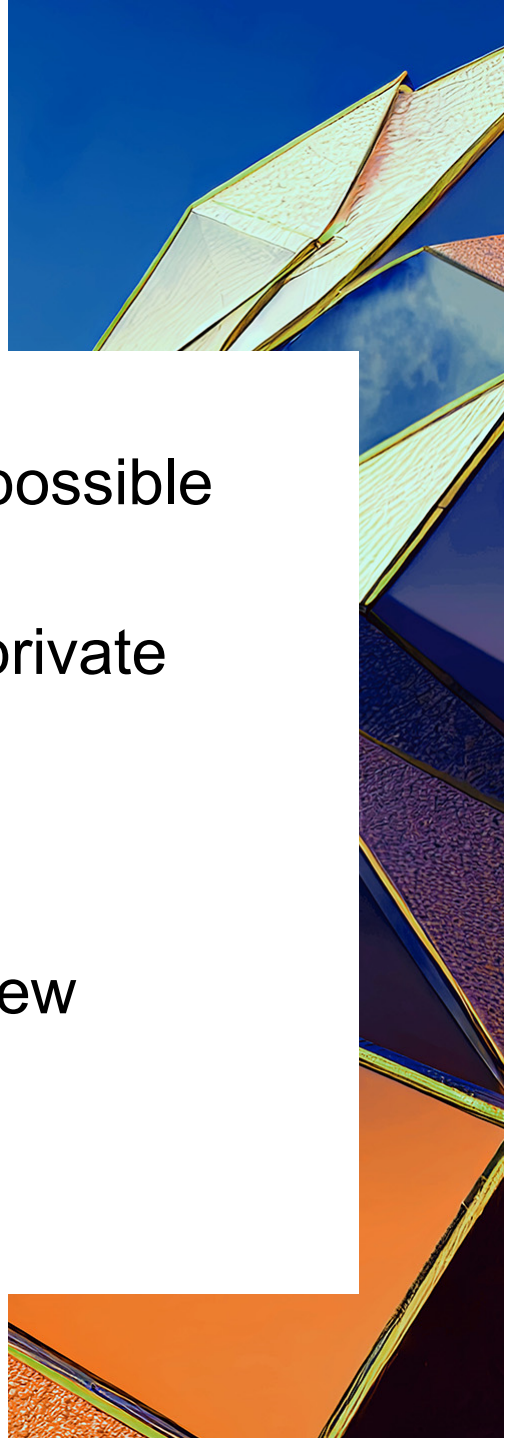
- Increased scrutiny of interlocking directorates and more Section 8 enforcement actions
  - FTC Chair Lina Khan described the Quantum/EQT complaint as part of an effort “to reactivate Section 8”
  - Expect FTC to bring similar cases going forward
- Section 8 is likely to be applied regardless of corporate form
  - Section 8 by its terms prohibits interlocks among competing “corporations”
  - But Quantum was not a corporation but a limited partnership
  - Chair Khan said the action “puts industry actors on notice that they must follow Section 8 no matter what specific corporate form their business takes”

2023 – Year in Review: Renewed Enforcement of Robinson-Patman Act



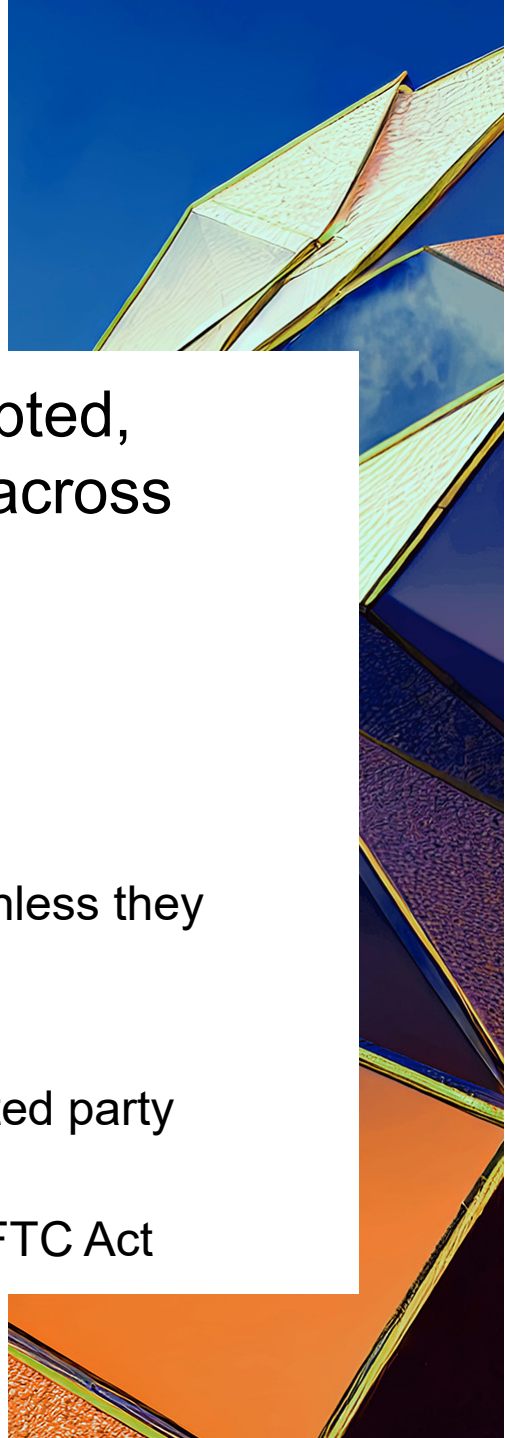
- In 1977, DOJ issued a report stating it would cease Robinson-Patman enforcement, in part because the law did not promote the antitrust goals of competition and low prices
- Recent statements and actions by the Biden Administration and FTC, however, suggest that a RPA revival is underway:
  - July 2021: Executive Order on Promoting Competition calls on FTC Chair to report on whether food industry practices may violate the RPA
  - September 2022: FTC Commissioner Alvaro M. Bedoya remarks that: "Certain laws that were clearly passed under what you could call a fairness mandate – ***laws like Robinson-Patman*** – directly spell out specific legal prohibitions. Congress's intent in those laws is clear. ***We should enforce them.***"
  - **January 2023:** Press reports that food and beverage companies are under investigation by the FTC over potential price discrimination in soft drink market
  - **March 2023**: Follow-on report that FTC has opened an investigation into a distributor for possible RPA violations based on better pricing for large retailers
  - **October 2023:** In the same investigation, FTC moved a federal court to enforce a civil investigative demand issued to one of the large retailers alleged to have received preferential pricing. The retailer refused to search employees' custodial files for responsive documents. A show-cause hearing has been scheduled.

2024 Outlook: Renewed Enforcement of Robinson-Patman Act



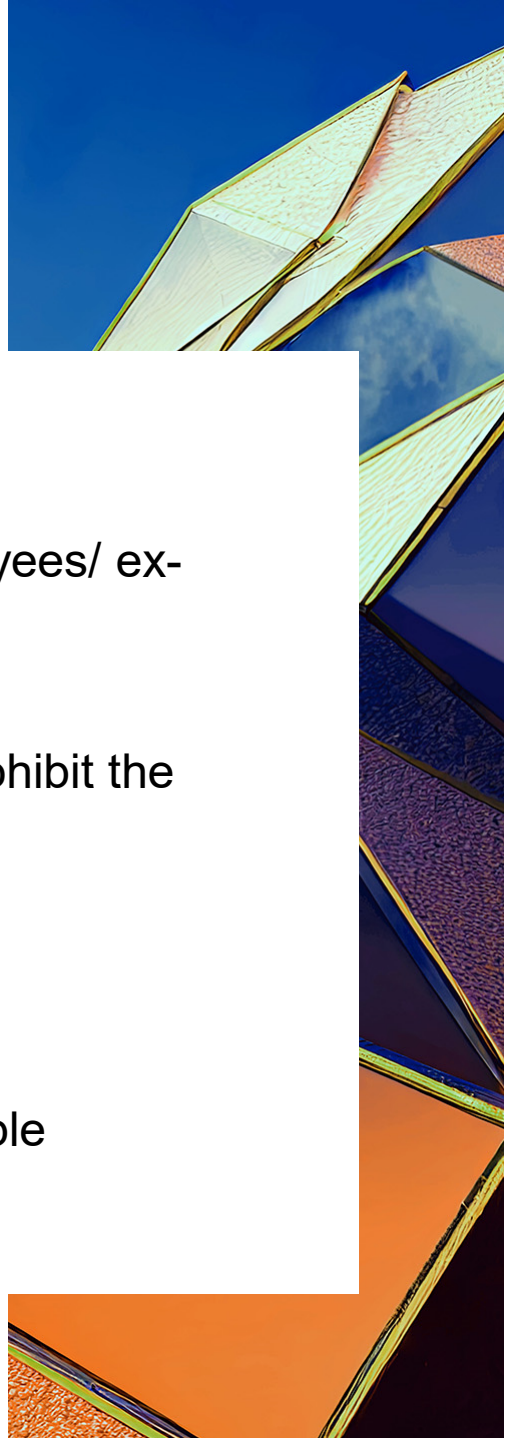
- Expect additional investigations into potential RPA violations and possible enforcement actions
- As is often the case, investigations may lead to a proliferation of private lawsuits
- Already seeing more private plaintiffs include RPA claims in their complaints
- Much of the RPA case law is from the twentieth century; look for new developments as more of these cases are litigated

2023 – Year in Review: Antitrust in Labor Markets (Employee Non-Competes)



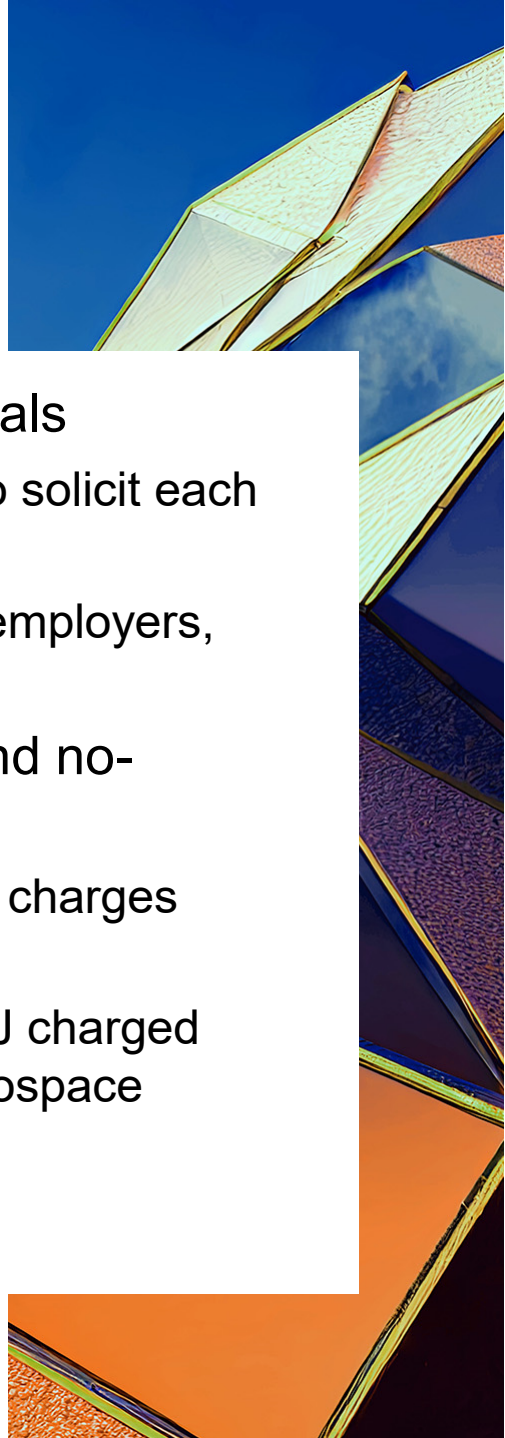
- **January 2023:** FTC announces a proposed regulation that, if adopted, would essentially abolish employee non-competition agreements across the United States
- Key features of proposed regulation include:
  - Ban on employee non-competes in almost all circumstances
  - Contemplated exemptions include:
    - Other forms of agreements with employees (e.g., non-disclosure/non-solicitation) unless they constitute a "*de facto*" non-compete
    - Non-employment related non-competes (e.g., business-to-business)
    - Non-competes in connection with sale of business or business unit provided restricted party owns >25% of the business or business unit being sold
    - Non-profits "<u>may</u> not be subject" to the rule to the extent they are exempt from the FTC Act

2023 – Year in Review: Antitrust in Labor Markets (Employe Non-Competes)



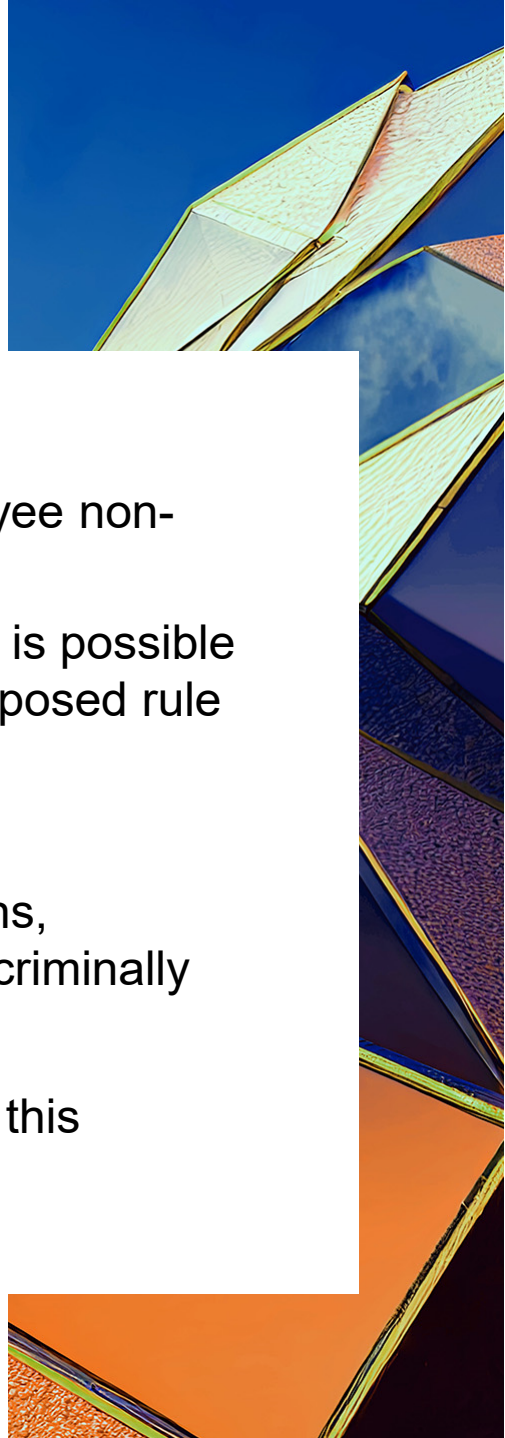
- Key features of proposed regulation include:
  - Prohibition on non-competes going forward and retroactively
    - Employers with existing non-competes must rescind agreements and inform employees/ ex-employees that the agreements are no longer valid
  - Preemption of inconsistent state laws
    - Even if the non-compete complies with state law, the proposed regulation would prohibit the agreement anyway
- When would this go into effect?
  - Not immediately
    - Public comment period now closed
    - FTC must adopt final rule, which will likely be subject to legal challenges and possible injunction
    - 180-day “compliance period” from publication before rule goes into effect

2023 – Year in Review: Antitrust in Labor Markets (No-Poach, No-Hire, and Wage-Fixing Agreements)



- October 2016: DOJ and FTC release joint antitrust guidance for HR professionals
  - "Naked" agreements between companies to fix wages or benefits, not to hire, or not to solicit each other's employees viewed as *per se* unlawful and subject to criminal prosecution
  - If restriction is reasonably necessary to a larger legitimate collaboration between the employers, the agreement will not be considered *per se* unlawful
- DOJ began prosecuting companies and individual executives for wage-fixing and no-poach / non-solicitation agreements with competitors
  - DOJ has failed to win a single jury conviction on any no-poach or wage-fixing criminal charges filed since 2020 (though it did obtain a pair of plea deals)
    - In April 2023, the court granted defendants' motion to acquit six executives that DOJ charged with a conspiracy to restrict the recruitment and hiring of engineers between an aerospace company and engineering staffing companies
    - Recently, DOJ abandoned its last remaining no-poach prosecution

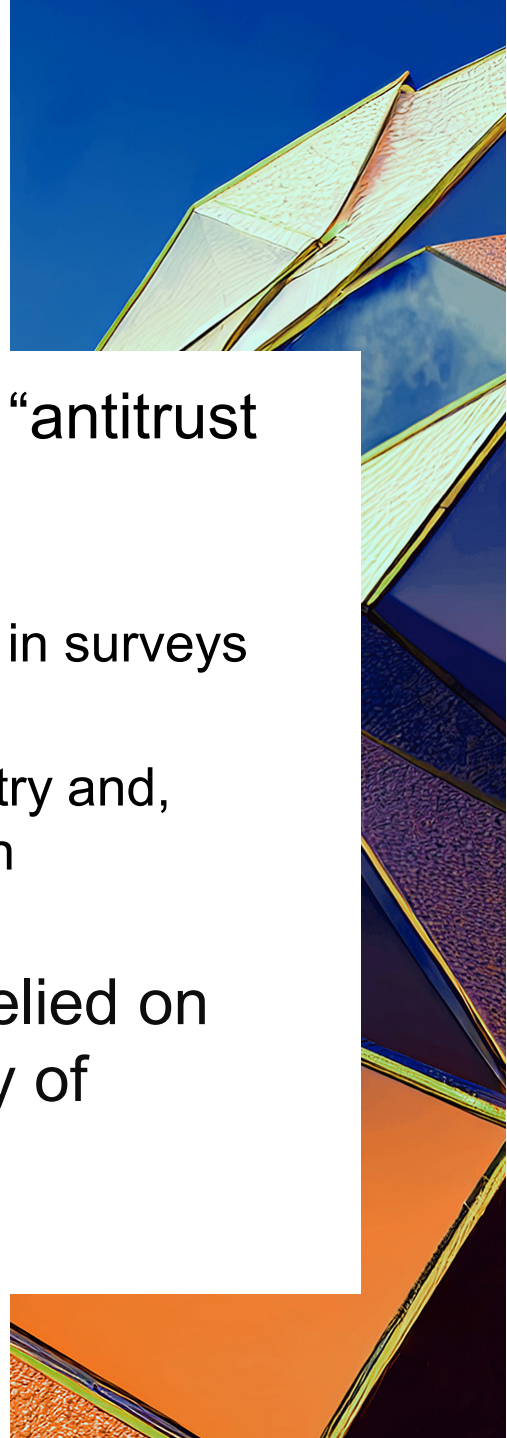
2024 Outlook: Antitrust in Labor Markets



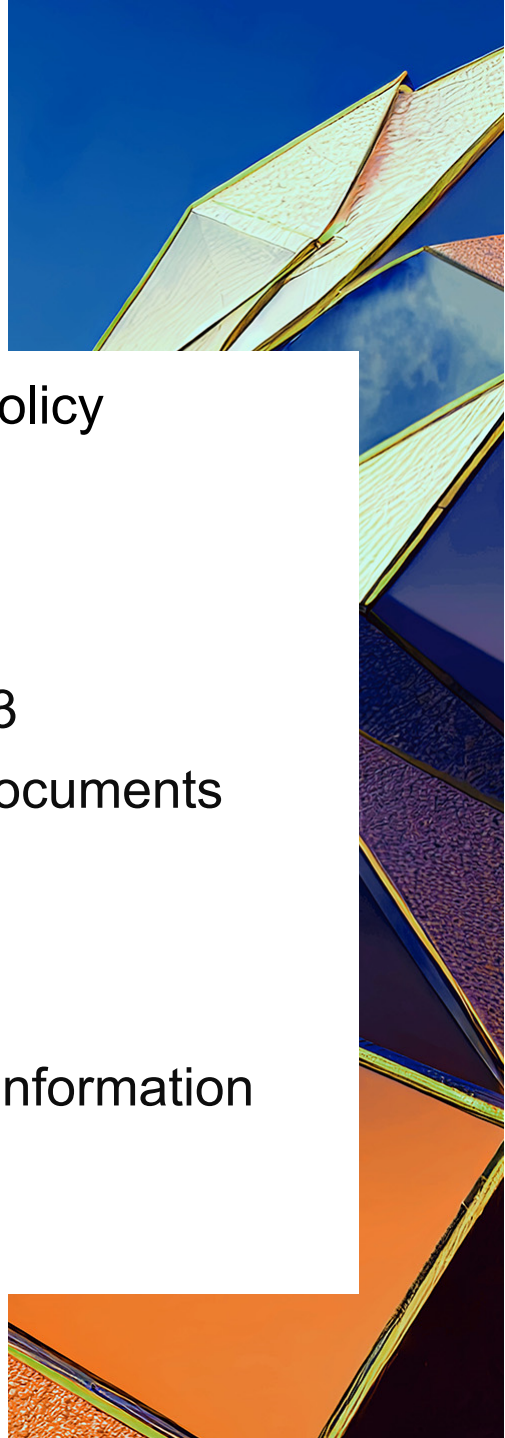
- Employee Non-Competes:
  - FTC is expected to vote in April 2024 on the final version of its proposal to ban employee non-compete agreements
  - Given recent administrative enforcement actions aimed at employee non-competes, it is possible that the FTC will challenge a company's non-compete provisions, even before the proposed rule is published (and regardless of the scope of the final rule)
- No-Poach, No-Hire, and Wage-Fixing Agreements
  - Given DOJ's lack of success in challenging no-poach agreements as criminal violations, companies can expect to see fewer (if any) of these types of cases being challenged criminally
    - However, DOJ may start to challenge these cases civilly
    - Private litigation is also likely to continue as private plaintiffs have been challenging this conduct with high success rates (e.g., *Deslandes* Seventh Circuit decision)
  - Criminal wage-fixing cases are still a risk area for companies in 2024

2023 – Year in Review: Withdrawal from Policy Statements on Information Sharing

- *1996 Statements of Antitrust Policy in Health Care* established an "antitrust safety zone" for certain exchanges of price and cost information
  - The safe harbor assured the business community that, absent "extraordinary circumstances," DOJ would not challenge health care providers' participation in surveys about prices or employee compensation if satisfied certain criteria
  - The policy statements relate to antitrust enforcement in the health care industry and, among other things, address the permissibility of information sharing between competitors
- Although related to health care, companies across the economy relied on these statements to share information with competitors in a variety of contexts



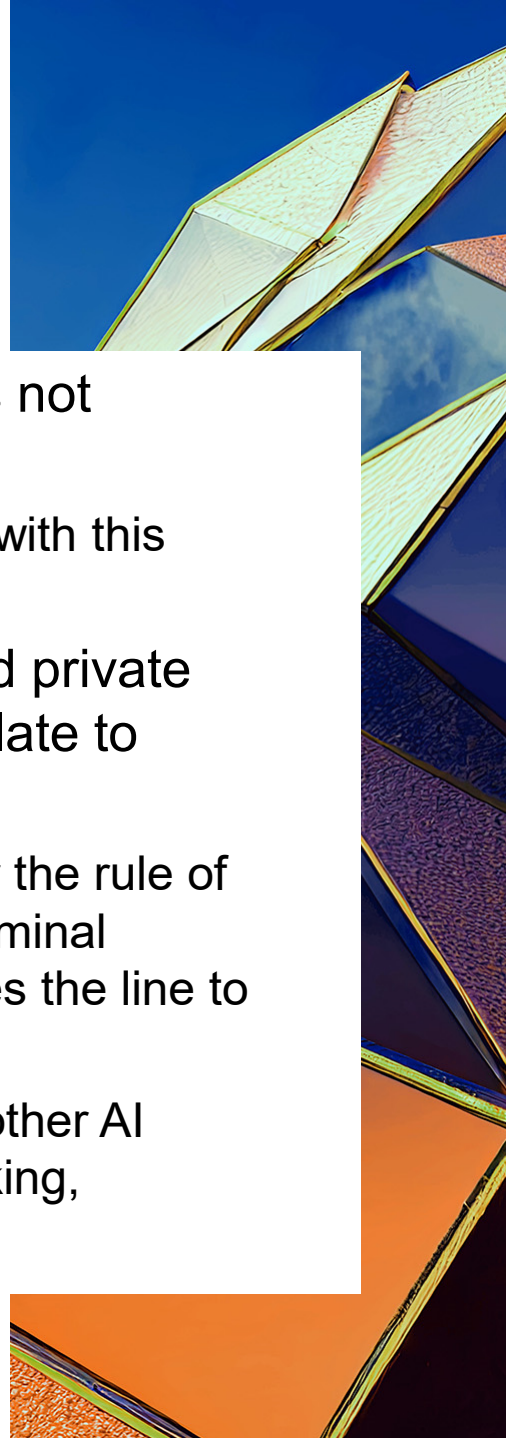
2023 – Year in Review: Withdrawal from Policy Statements on Information Sharing



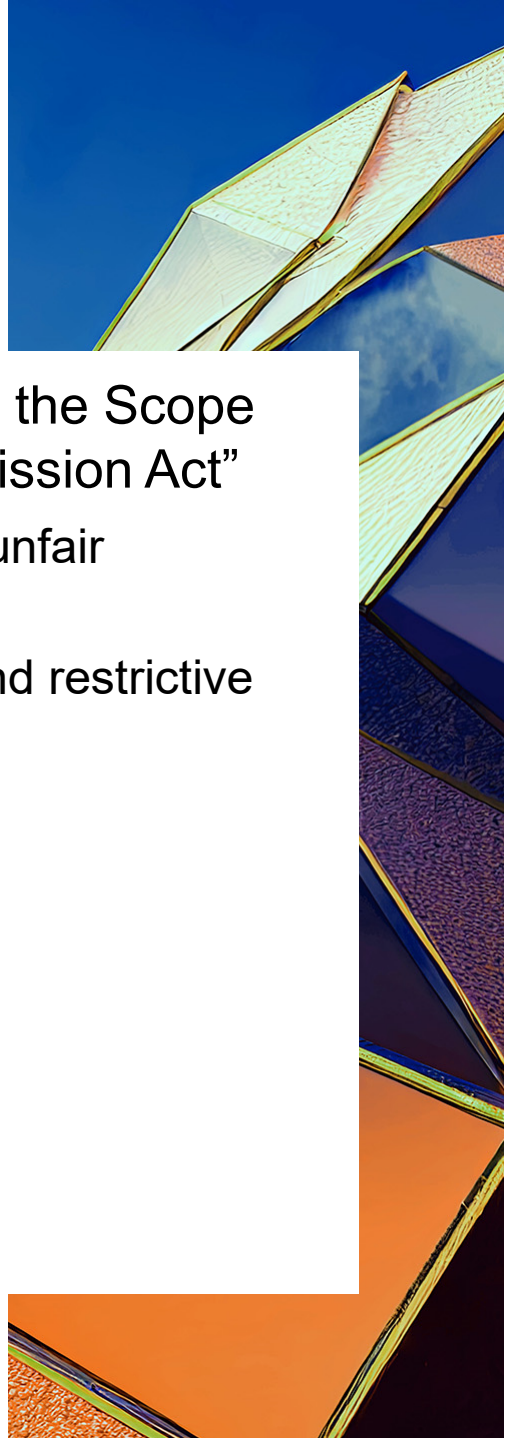
- **February 2023:** DOJ Antitrust Division announces that it is withdrawing three policy statements DOJ and FTC issued between 1993 and 2011
- DOJ has not said whether it will replace the withdrawn policy statements
- Taking a "case-by-case enforcement approach"
- FTC joined the DOJ in withdrawal of two of these policy statements in July 2023
- The statements are cited in other, broadly applicable DOJ and FTC guidance documents that have not been withdrawn:
  - 2016 DOJ/FTC *Antitrust Guidance for Human Resource Professionals*
  - DOJ/FTC *Antitrust Guidelines for Collaborations Among Competitors*
- In September 2023, the DOJ and several states filed a Section 1 Sherman Act information sharing enforcement action against Agri Stats, Inc.

2024 Outlook: Withdrawal from Policy Statements on Information Sharing

- Conduct that was permissible under the now-withdrawn policy statements does not suddenly become illegal
  - But companies should take a fresh look at their information exchange arrangements with this development in mind as they move into 2024
- Expect more aggressive agency enforcement in this space going into 2024, and private follow-on lawsuits are also likely to follow these enforcement actions as they relate to information-sharing practices
  - While information exchange claims under the Sherman Act tend to be analyzed under the rule of reason, DOJ civil investigations of such conduct have the potential to spillover into criminal enforcement in cases where the exchange of information between competitors crosses the line to agreements to fix prices
  - Companies should expect that the agencies will scrutinize the use of algorithms and other AI technology that may help companies predict competitors' strategies and decision-making, particularly when they rely on data collected from competitors



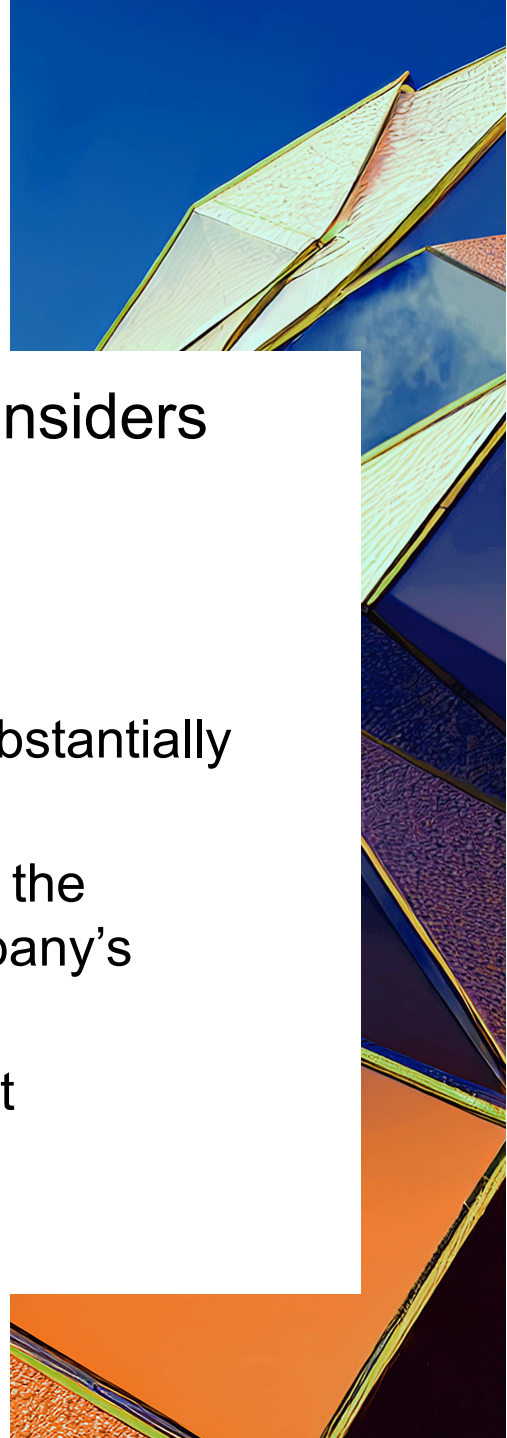
2023 – Year in Review: FTC's Expansion of Power Under Section 5



- On November 10, 2022, the FTC released a new "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act"
  - Reflects significant expansion of the scope of what the FTC considers to constitute "unfair methods of competition" prohibited by Section 5 of the FTC Act
  - Takes the position that Section 5 reaches methods of competition that are abusive and restrictive
    - Even if the conduct does not otherwise violate the Sherman or Clayton Acts
    - Even if the conduct does not actually harm competition or consumers
- "Method of competition" = conduct by an actor in the marketplace
  - NOT conditions in the marketplace (i.e., high barriers to entry or high concentration)
  - Effect on competition can be direct or indirect
- "Unfair" = conduct that goes beyond competition on the merits

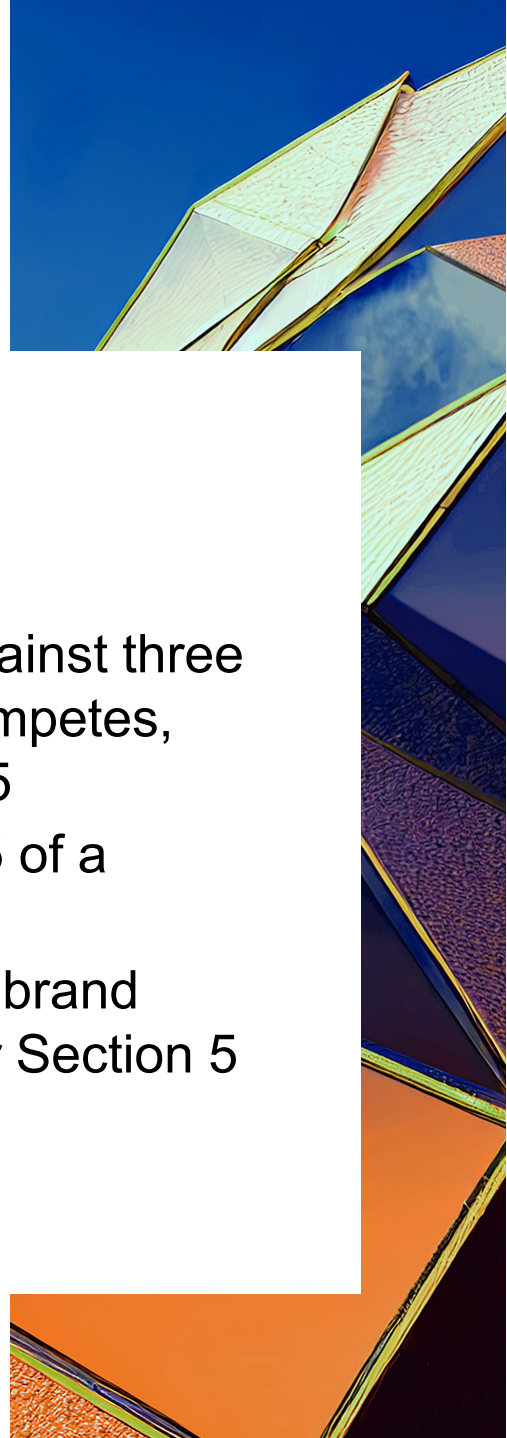
2023 – Year in Review: FTC's Expansion of Power Under Section 5

- Includes 20 non-exhaustive categories of conduct that the FTC considers "unfair methods of competition"
  - Invitations to collude
  - Practices that facilitate tacit coordination
  - A series of mergers, acquisitions, or joint ventures that individually do not "substantially lessen competition" but have an aggregate unfair effect
  - Loyalty rebates, tying, bundling, or exclusive dealing arrangements that have the tendency to ripen into antitrust violations due to industry conditions or a company's position within the industry
  - Interlocking directorates not covered by the literal language of the Clayton Act

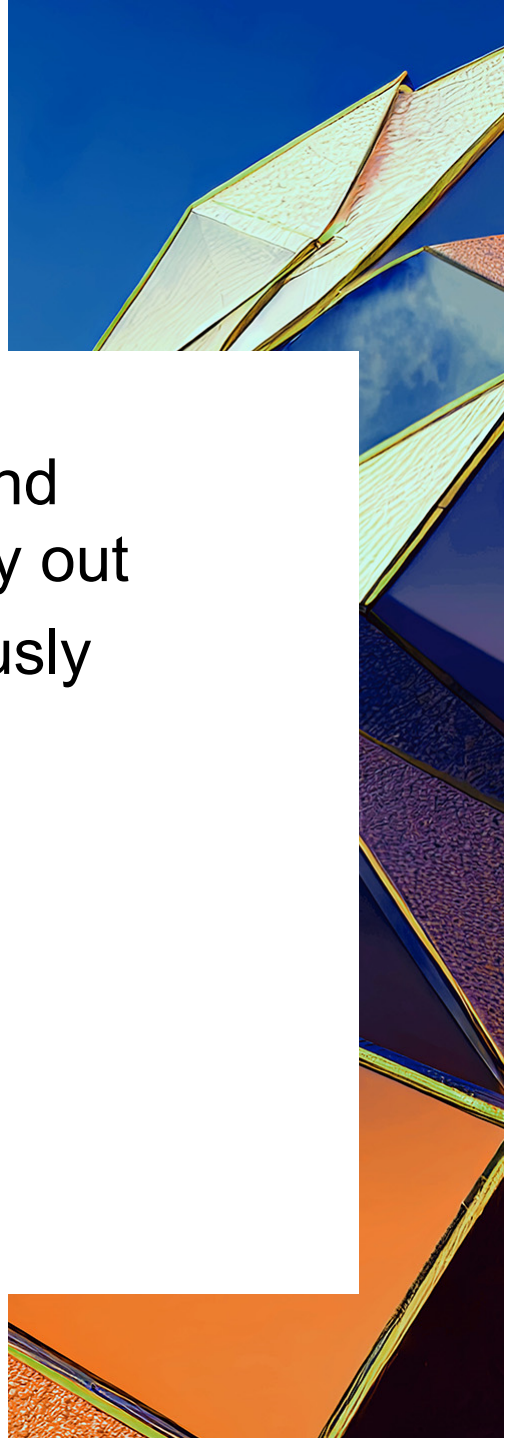


2023 – Year in Review
FTC's Expansion of Power Under Section 5

- The Policy Statement is a deliberate move to expand the FTC's enforcement authority
- In 2023, FTC began testing the waters:
  - **January 2023:** FTC filed administrative lawsuits and reached settlements against three companies and two individuals for requiring employees to sign broad non-competes, which the FTC alleged was an "unfair method of competition" under Section 5
  - **February 2023**: CIDs issued in connection with investigation under Section 5 of a distributor
  - **Fall 2023:** FTC policy statement related to improper Orange Book listings by brand name pharmaceutical companies, cautioning these may be challenged under Section 5 of the FTC Act

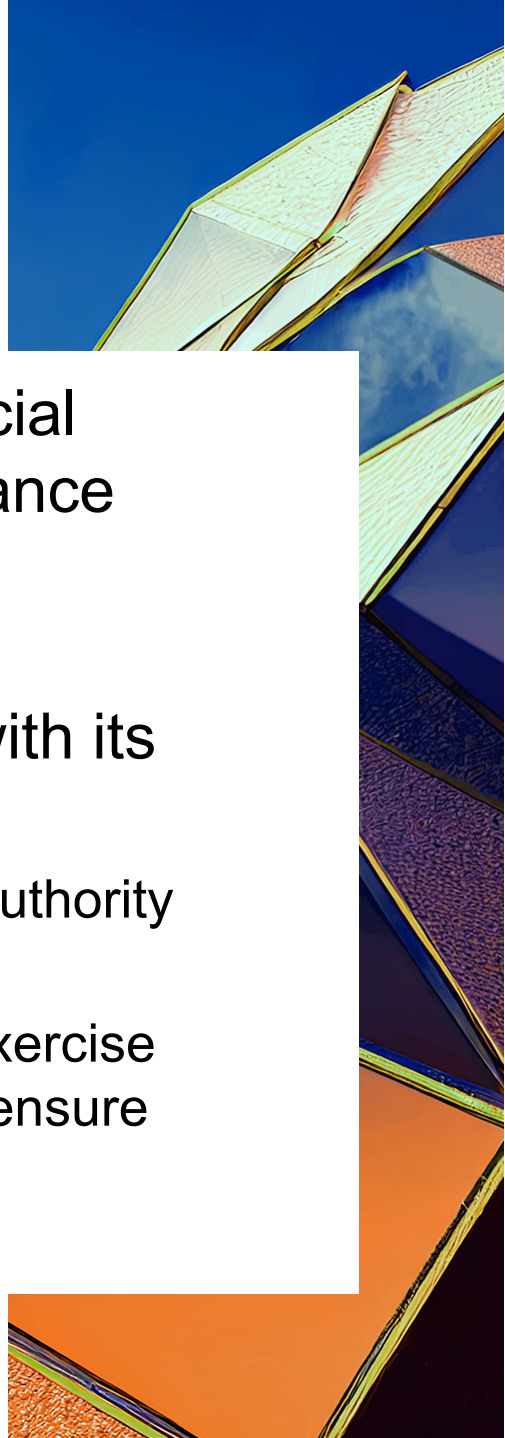


2024 Outlook
FTC's Expansion of Power Under Section 5



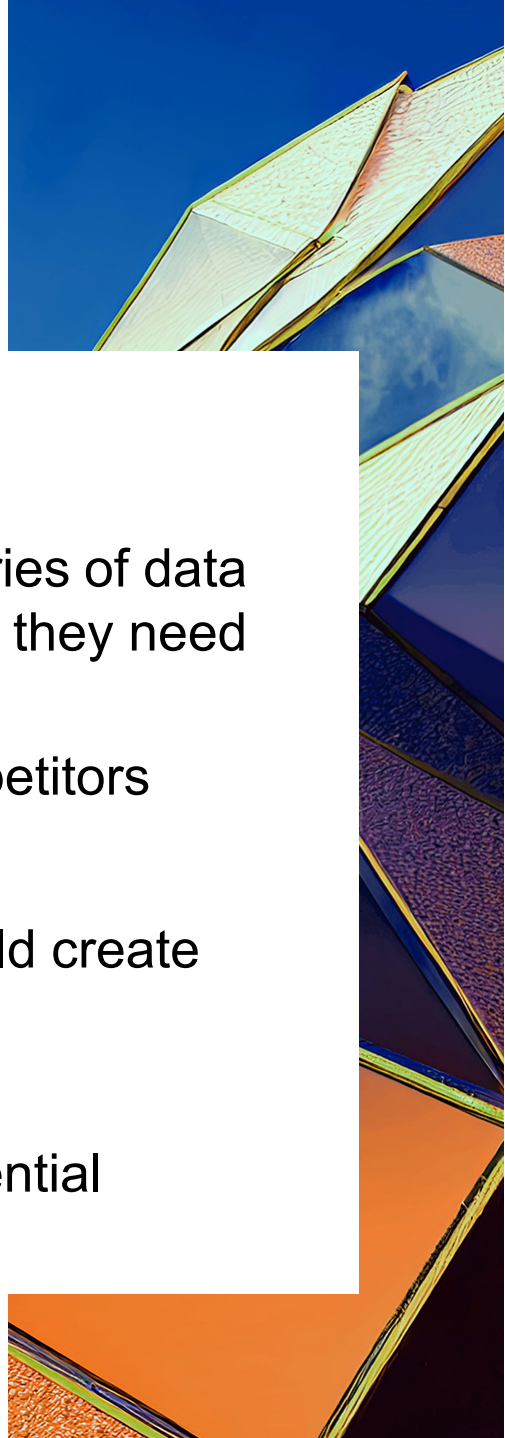
- Ultimately, courts will decide if the Policy Statement reflects a sound interpretation of the FTC's authority, which could take years to play out
- Expect to see increased FTC activity aimed at conduct not previously challenged under the antitrust laws

2023 – Year in Review: What Antitrust Means for Artificial Intelligence



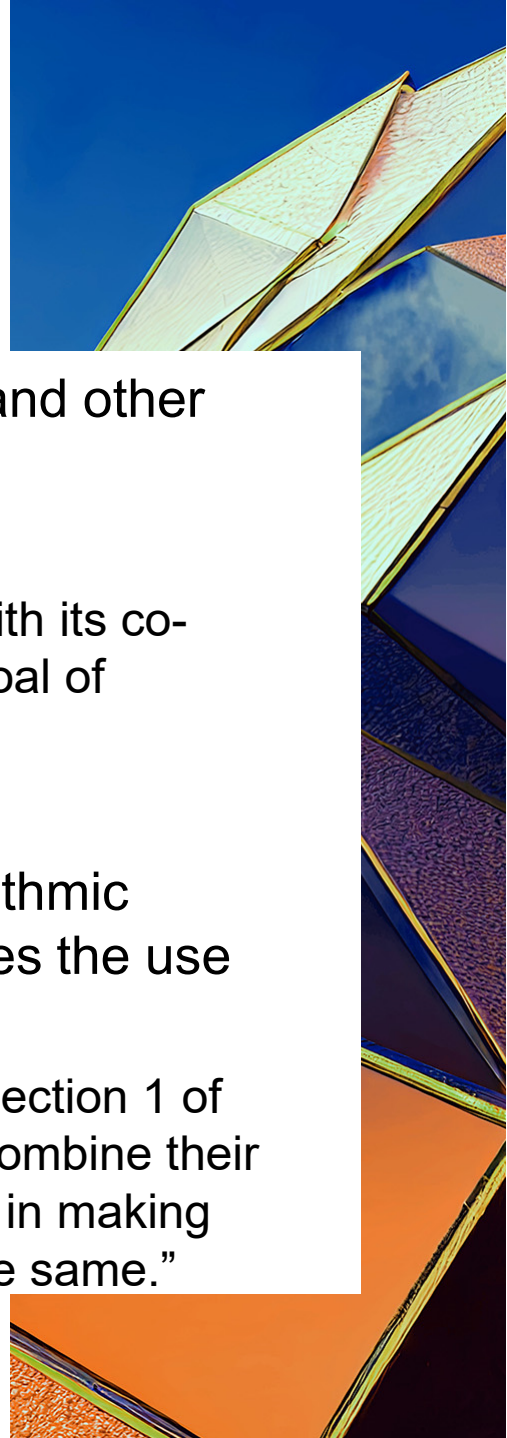
- Companies across numerous industries are increasingly using artificial intelligence (AI) to create innovations, compete with rivals, and enhance overall performance
- At the same time, antitrust enforcers are finding new ways to apply antitrust laws to AI. The Biden Administration has also weighed in with its recent Executive Order on AI, announced on October 30
  - The FTC has repeatedly expressed its willingness/ability to utilize its statutory authority to regulate novel uses of AI, including those that negatively affect competition
  - The Biden Executive Order also encouraged the FTC to consider "whether to exercise the Commission's existing authorities, including its rulemaking authority . . . to ensure fair competition in the AI marketplace"

2023 – Year in Review: What Antitrust Means for Artificial Intelligence



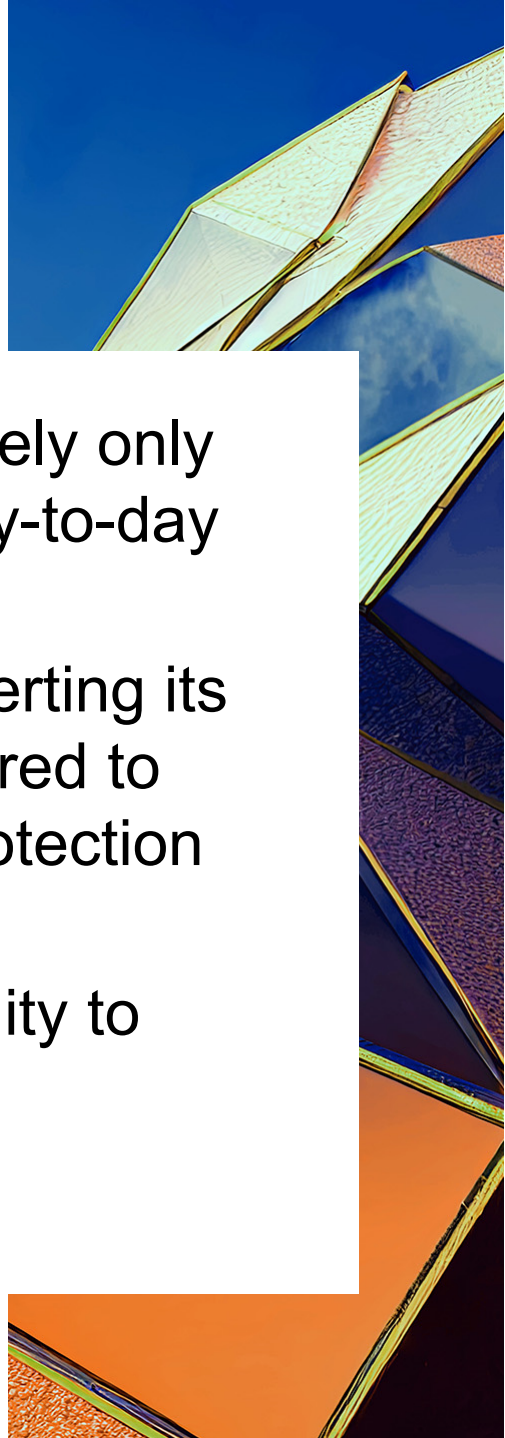
- Mergers:
  - Antitrust enforcers looking at how mergers may combine powerful repositories of data or market intelligence or deprive customers and competitors of critical tools they need to compete
  - Includes scrutiny of both vertical mergers and acquisitions of nascent competitors
- Conduct:
  - AI tools may create information asymmetries or power imbalances that could create unfair competitive advantages
  - Some argue AI could be a tool for facilitating collusion
  - AI-related standard-setting and the potential for foreclosure of rivals or potential disrupters from fully competing on the merits

2023 – Year in Review: What Antitrust Means for Artificial Intelligence (Algorithmic Pricing)



- Businesses are increasingly using algorithms to make decisions about pricing and other matters
- In recent years, the practice has begun to attract regulatory scrutiny
  - For example, in 2016, DOJ secured a guilty plea from an online retailer that agreed with its co-conspirators to adopt specific pricing algorithms for the sale of wall posters with the goal of coordinating price changes
- Private plaintiff's antitrust bar is pursuing similar cases
- **November 2023:** DOJ filed a statement of interest in a large, multidistrict algorithmic pricing case setting forth the Department's view that under certain circumstances the use of an algorithm to set prices can be per se illegal:
  - "Although not every use of an algorithm to set price qualifies as a per se violation of Section 1 of the Sherman Act, it is per se unlawful when, as alleged here, competitors knowingly combine their sensitive, nonpublic pricing and supply information in an algorithm that they rely upon in making pricing decisions, with the knowledge and expectation that other companies will do the same."

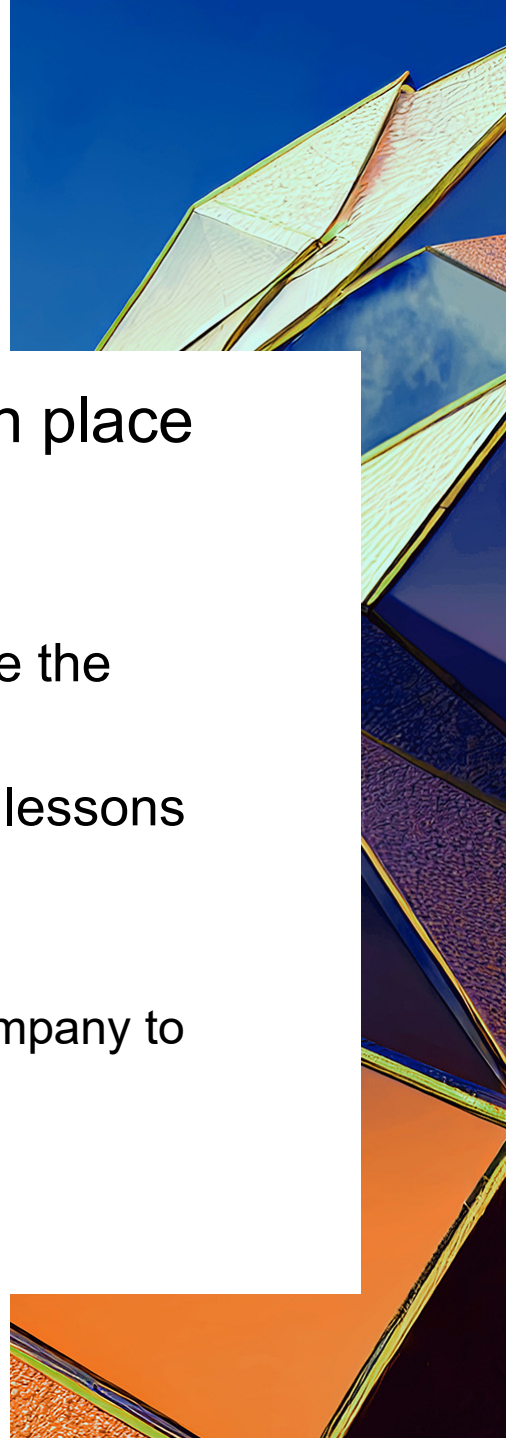
2024 Outlook:
What Antitrust Means for Artificial Intelligence



- AI is quickly evolving, and enforcement of the antitrust laws will likely only increase as AI becomes even more integrated into companies' day-to-day operations
- Expect to see agencies like the FTC, which has already been asserting its existing authority to address AI issues, to feel even more empowered to bring enforcement actions under its competition and consumer protection authority
- Expect to see the agencies *deploying* AI tools to improve their ability to oversee competition in the U.S. economy

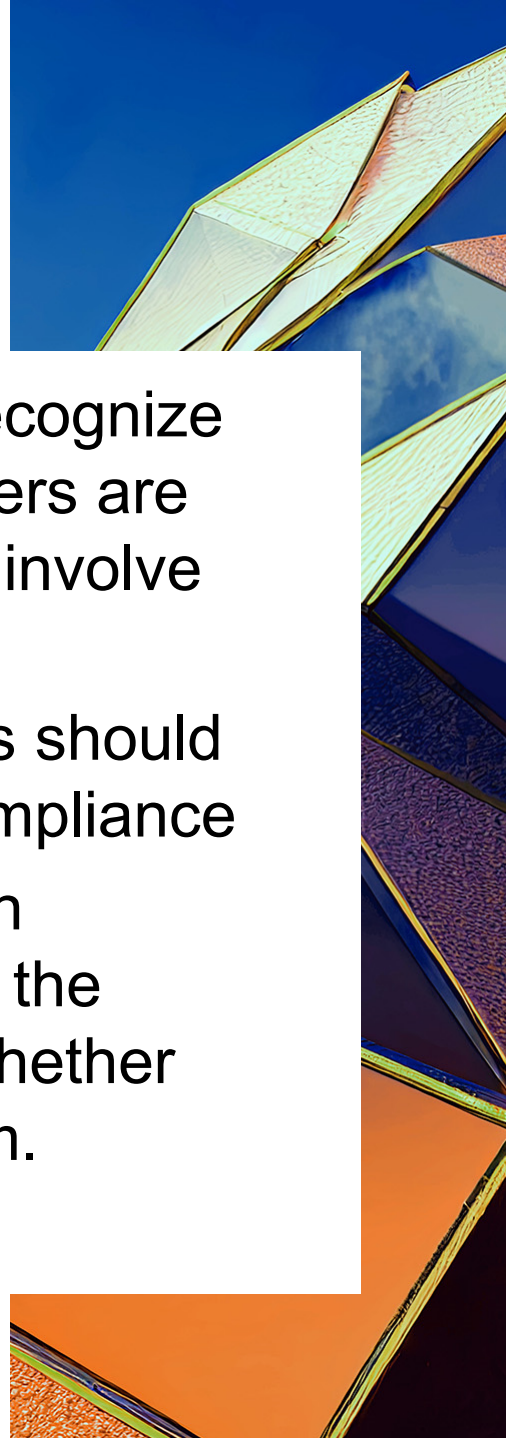
Best Practices to Reduce Antitrust Risk

- Companies should have effective antitrust compliance programs in place to deter and detect anticompetitive conduct
  - "Off the Shelf" programs will not cut it
  - Need to adapt compliance program to fit the company's risk profile and evolve the program over time
  - Companies should be updating policies based on periodic risk assessments, lessons learned, and changes to DOJ/FTC regulations and guidance
  - Auditing and testing should be components of the compliance program
    - Could include review of documents or communications in high-risk areas for the company to help detect or deter problematic conduct



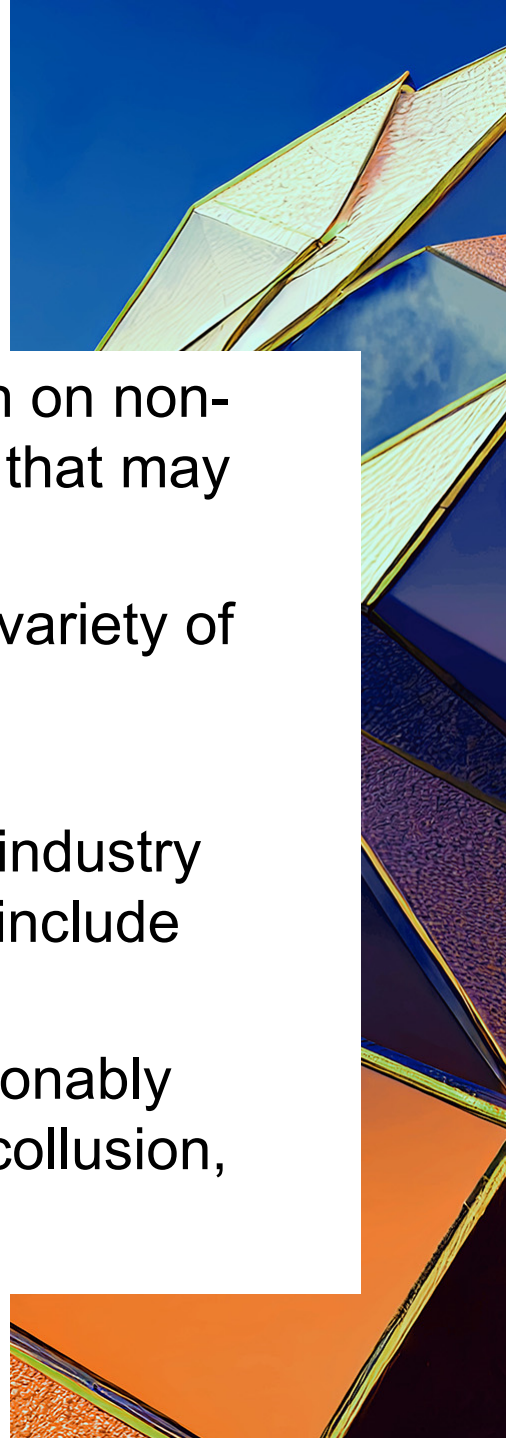
Best Practices to Reduce Antitrust Risk

- Companies contemplating vertical or horizontal mergers should recognize that such transactions may soon be presumptively illegal, and others are likely to garner a harder look and possibly an outright challenge – involve antitrust counsel early
- In response to revived Robinson-Patman enforcement, companies should review pricing policies and programs to ensure continued RPA compliance
- Companies should avoid sharing common officers or directors with competitors and take steps to verify no such interlocks exist given the reactivation of Section 8 enforcement. This is true regardless of whether the companies are corporations or take some other corporate form.



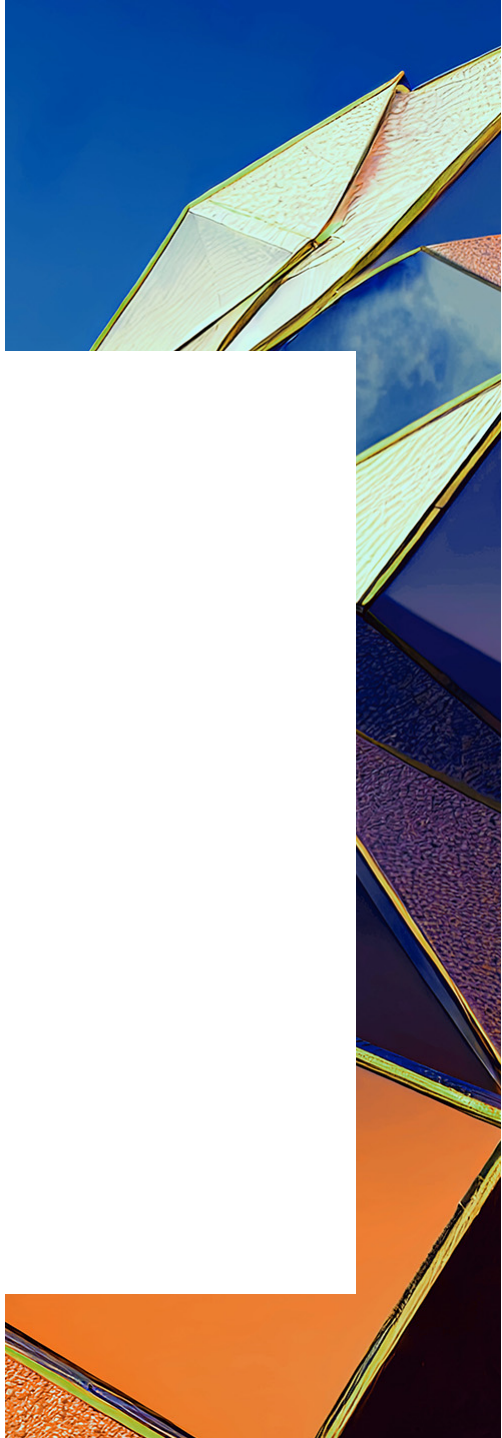
Best Practices to Reduce Antitrust Risk

- Companies should closely monitor the status of the FTC's proposed ban on non-compete agreements and work with counsel to identify any agreements that may not comply with the final rule
- Review your agreements – non-solicit provisions are very common in a variety of agreements. If you have them, evaluate the necessity and scope of the restriction.
- Companies should evaluate information exchanges and participation in industry surveys given the DOJ's withdrawal from related policy statements and include past instances of information sharing in their antitrust audits
- Companies should be mindful to ensure their AI practices do not unreasonably foreclose rivals, create unfair or coercive power asymmetries, facilitate collusion, or lead to unreasonably low standards of competition



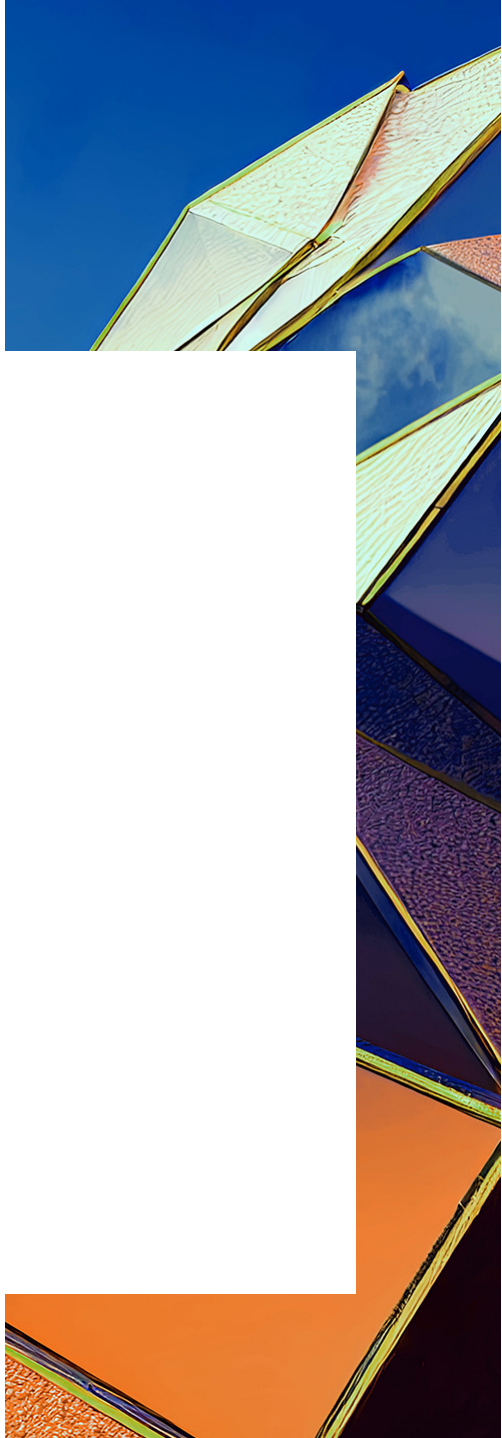
Thank You

- Questions?



About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.



FOLEY

FOLEY & LARDNER LLP

FOLEY.COM

FOLEY

FOLEY & LARDNER LLP

Break

Presentations will resume shortly

FOLEY

FOLEY & LARDNER LLP

Cybersecurity in Manufacturing and the Supply Chain

December 7, 2023

Presenters

Aaron Tantleff
Partner

T: 312.832.4367
E: atantleff@foley.com

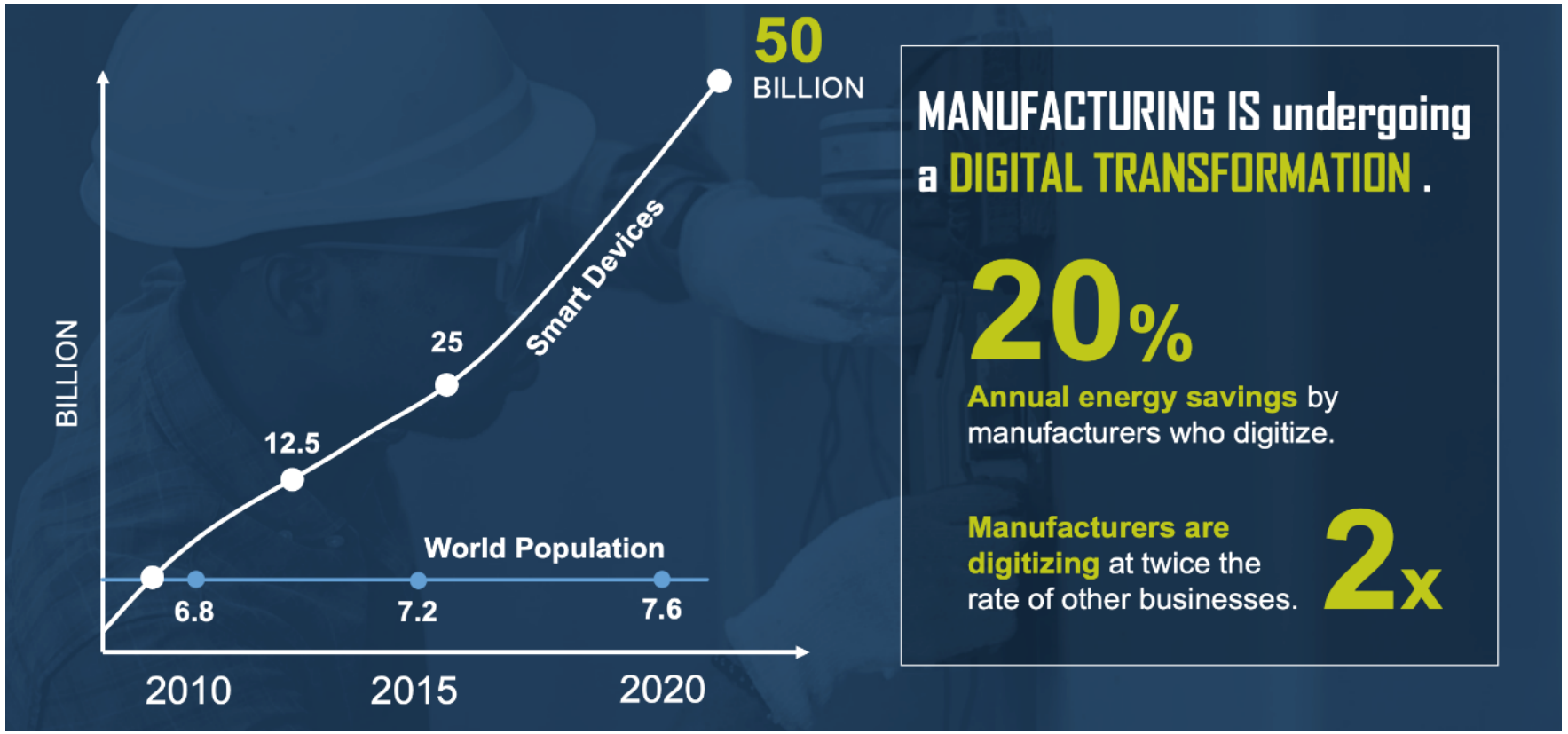
Howard Grimes, Ph.D.
Chief Executive Officer
Cybersecurity Manufacturing Innovation Institute
T: 509.432.4652
E: Howard.Grimes@cymanii.org

FOLEY

FOLEY & LARDNER LLP

How Did We Get Here?

Cyber Vulnerabilities are On the Rise – Exponentially



Bloomberg

US Edition

Live Now | Markets | Economics | Industries | Tech | AI | Politics | Wealth | Pursuits | Opinion | Businessweek

Opinion | Brooke Sutherland, Columnist

Manufacturers Move to the Front Line of Cyberattacks

The growing rate of hacks at industrial companies is an unpleasant byproduct of a surge of investment in digital connectivity.

November 8, 2023 at 11:35 AM CS

MANUFACTURING NET

VIDEO | ADVERTISE | NEWSLETTER SIGNUP | PODCAST

Aerospace | Artificial Intelligence | Automotive | **Cybersecurity** | Energy | Industry 4.0 | Operations | Software | Supply Chain

CYBERSECURITY

Manufacturing Segments that Face the Greatest Cyber Risks

Even as cybersecurity strategies improve each year, the sophistication of attacks and capabilities of hackers continue to rise.

By – Isla Sibanda

CYBERSCOOP

Ransomware attacks surge against US manufacturing plants

Cyberattacks against critical infrastructure continues to increase and some sectors, such as manufacturing, take the brunt of abuse.

BY CHRISTIAN VASQUEZ • FEBRUARY 14, 2023

#1 Trusted Cybersecurity News Platform

The Hacker News

Industrial Control Systems Vulnerabilities Soar: Over One-Third Unpatched in 2023

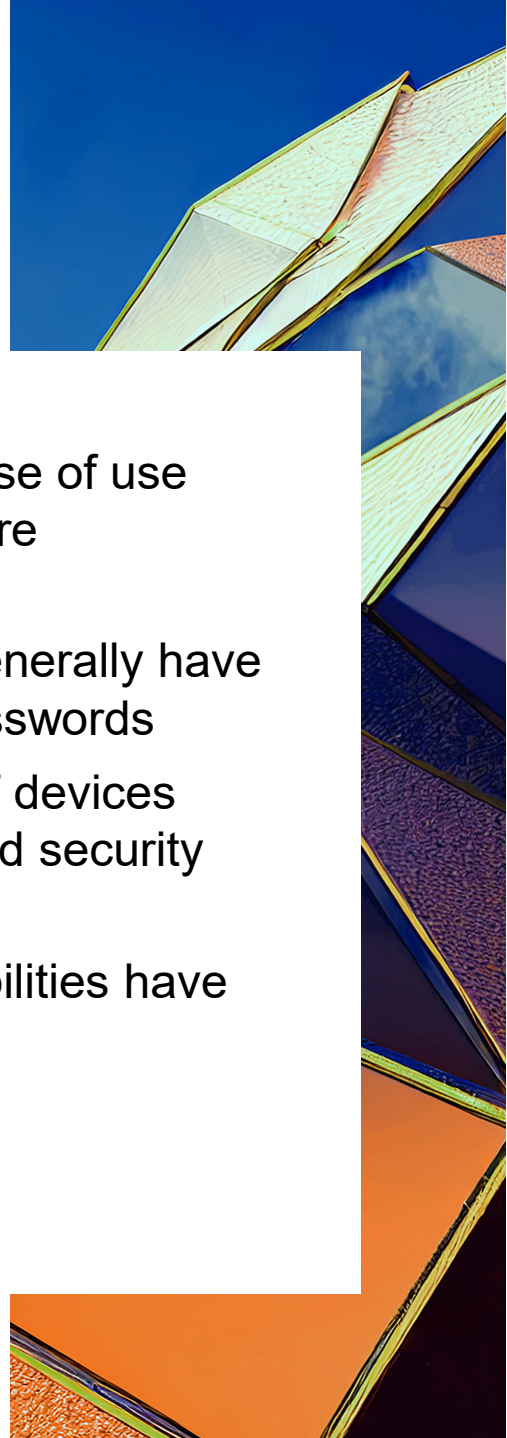
Aug 02, 2023 Newsroom

CVEs by CVSS Criticality, First Half of 2023

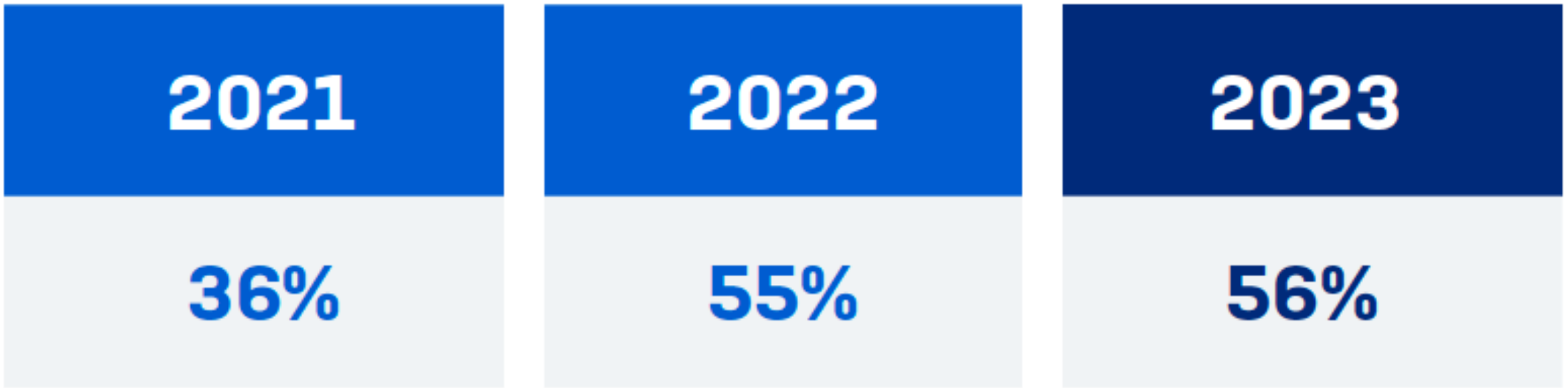
	1H 2023 Count	Percentage of Total (670)	1H 2022 Count	Percentage of Total (681)
Critical	88	13.1%	152	22.3%
High	349	52.1%	289	42.4%
Medium	215	32.1%	205	30.1%
Low	18	2.7%	35	5.1%
	High/Critical	65.2%	High/Critical	64.76%

IoT Cyber Attacks

- "Vulnerable by Design"
  - Systems not designed with security in mind
  - Increasing number of devices talking to each other creates a greater attack surface for cyber attackers to take advantage of
  - Hybrid and remote work environments, along with the proliferation of technology increases the risks posed by connecting or sharing data over improperly secured devices
- Many devices are designed for ease of use and convenience rather than secure operations
  - Consumer grade IoT devices generally have weak security protocols and passwords
  - Commercial/industrial grade IoT devices generally don't follow established security standards
  - Significant, well-known vulnerabilities have persisted for years



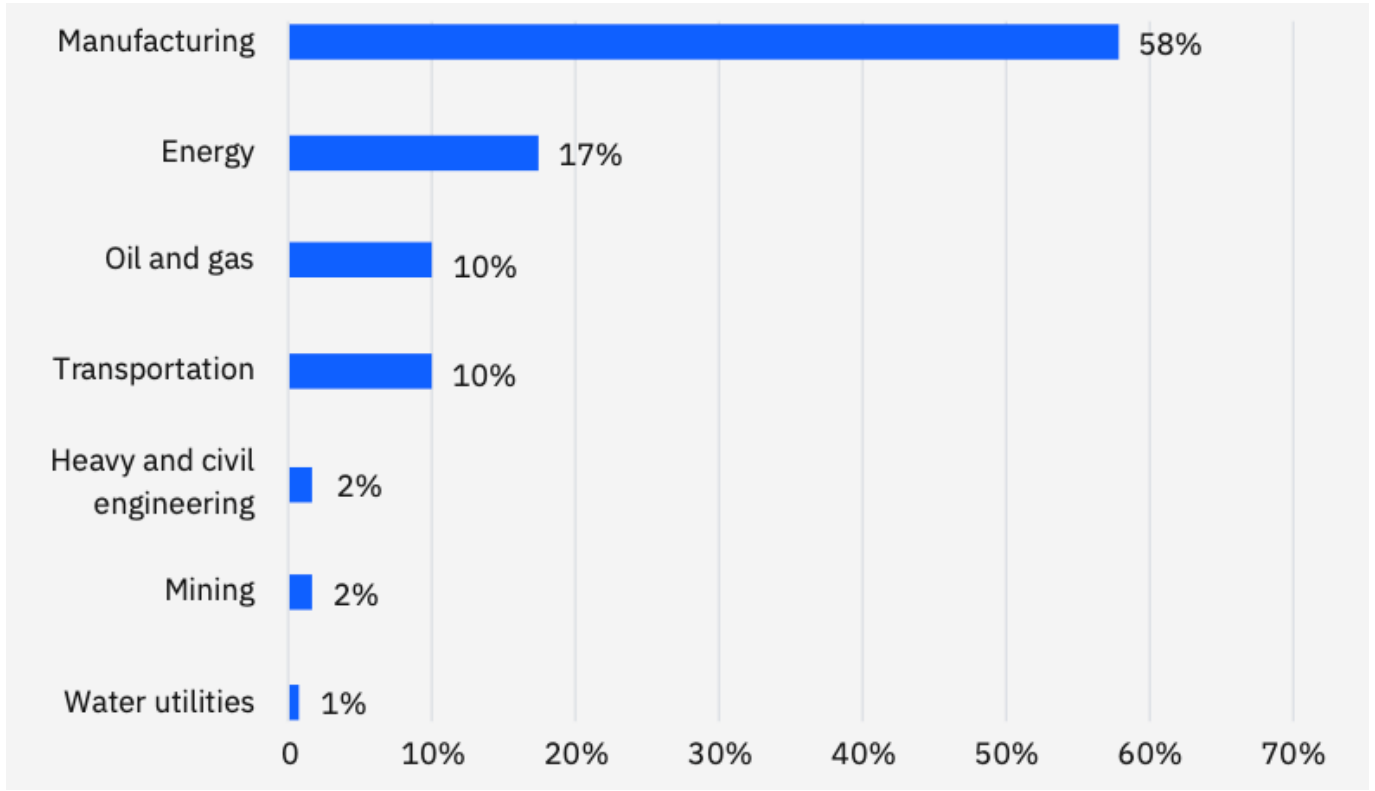
Rate of Ransomware Attacks in Manufacturing



In the last year, has your organization been hit by ransomware? Yes. n=363 (2023), 419 (2022), 438 (2021)

Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

Threats to OT and industrial control systems

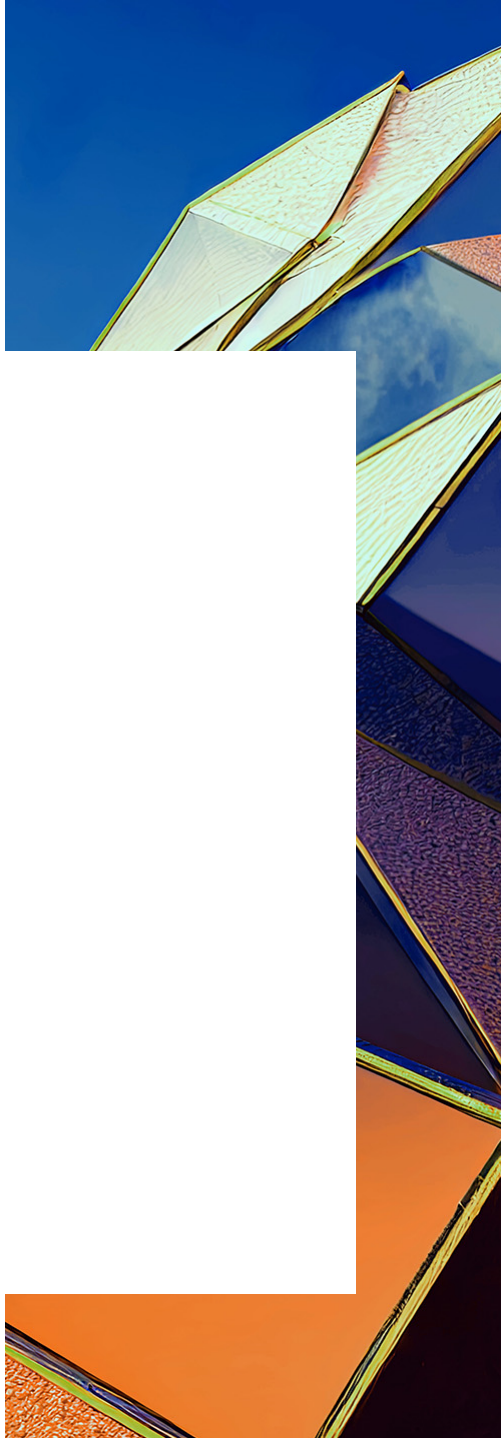


Source: X-Force Threat Intelligence Index 2023, IBM Security

* Proportion of IR cases by OT-related industry to which X-Force responded in 2022

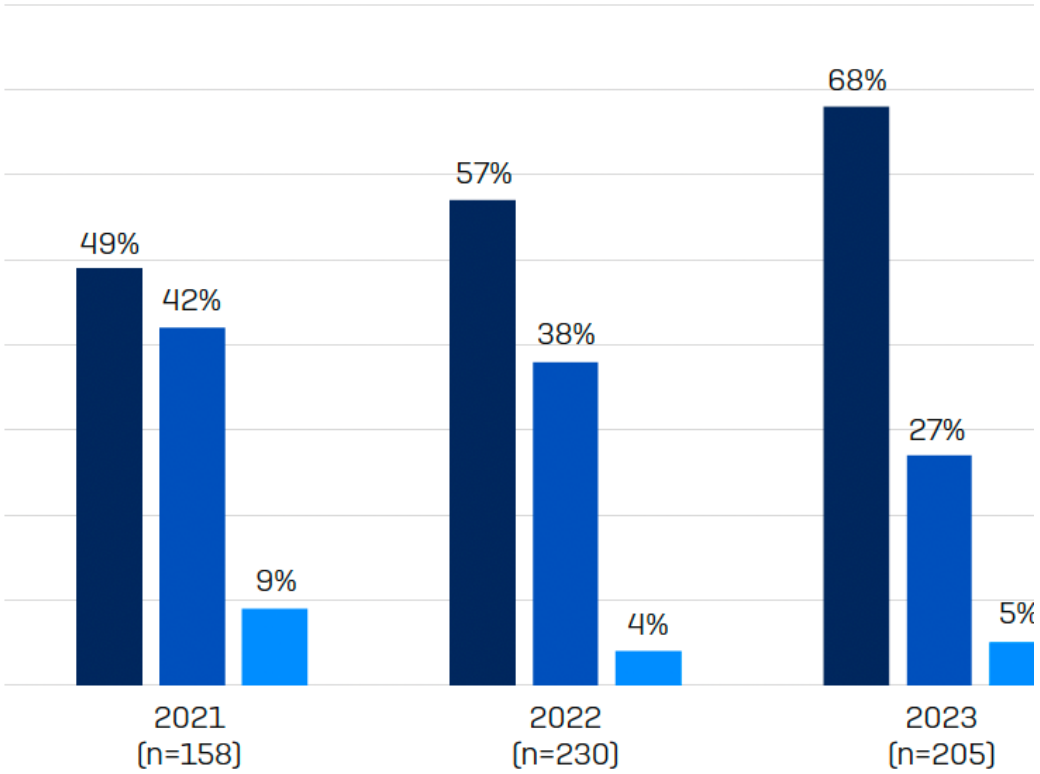
Root Causes of Ransomware Attacks in Manufacturing

	MANUFACTURING AND PRODUCTION	CROSS-SECTOR AVERAGE
Exploited vulnerability	24%	36%
Compromised credentials	27%	29%
Malicious email	21%	18%
Phishing	20%	13%
Brute force attack	5%	3%
Download	2%	1%



Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

Rate of Data Encryption in Manufacturing

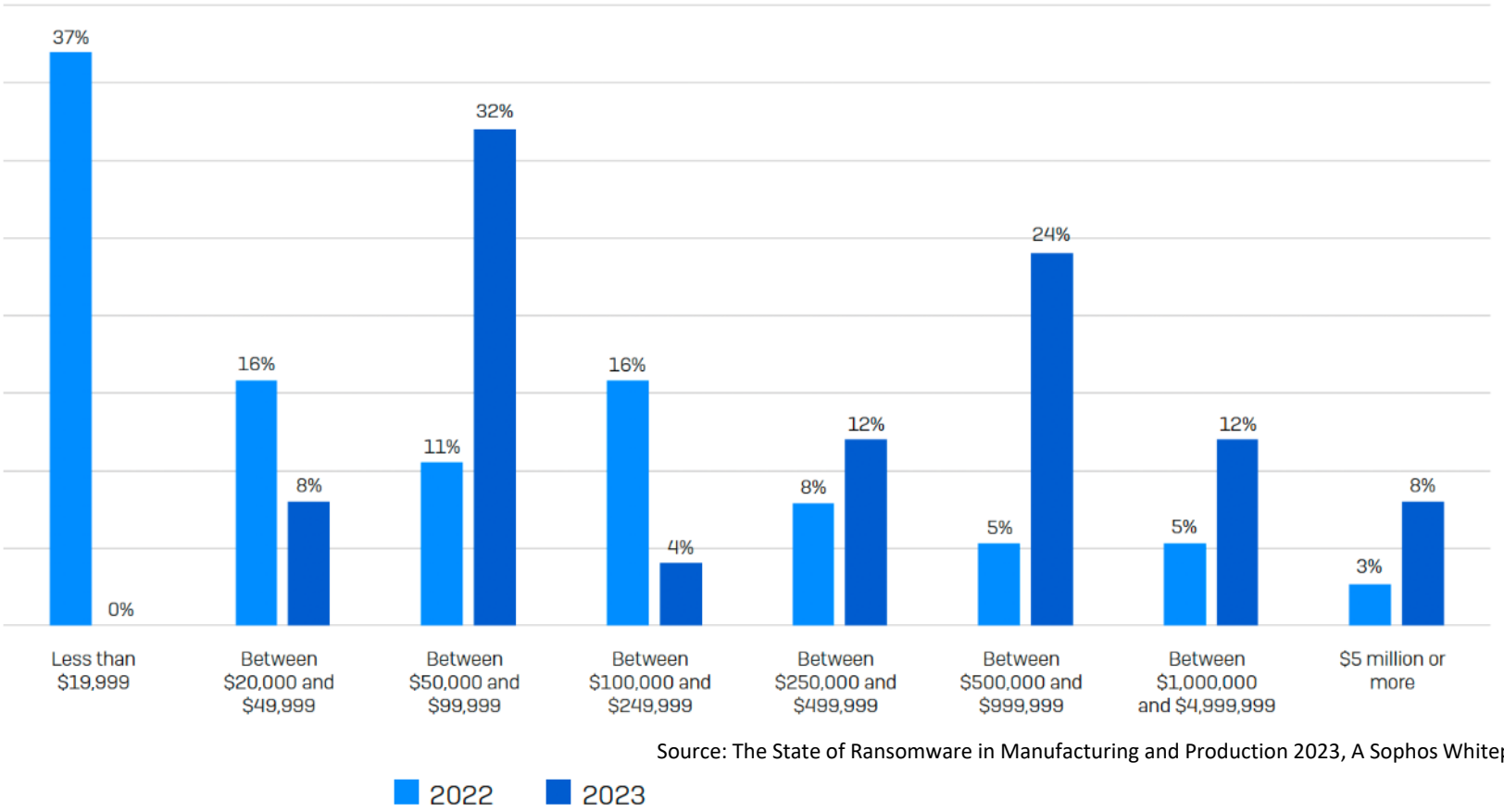


Yes - Data was encrypted
No - The attack was stopped before data was encrypted
No - Data was not encrypted but we were still held to ransom (extortion)

Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack?
Selection of answer options. Base numbers in chart

Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

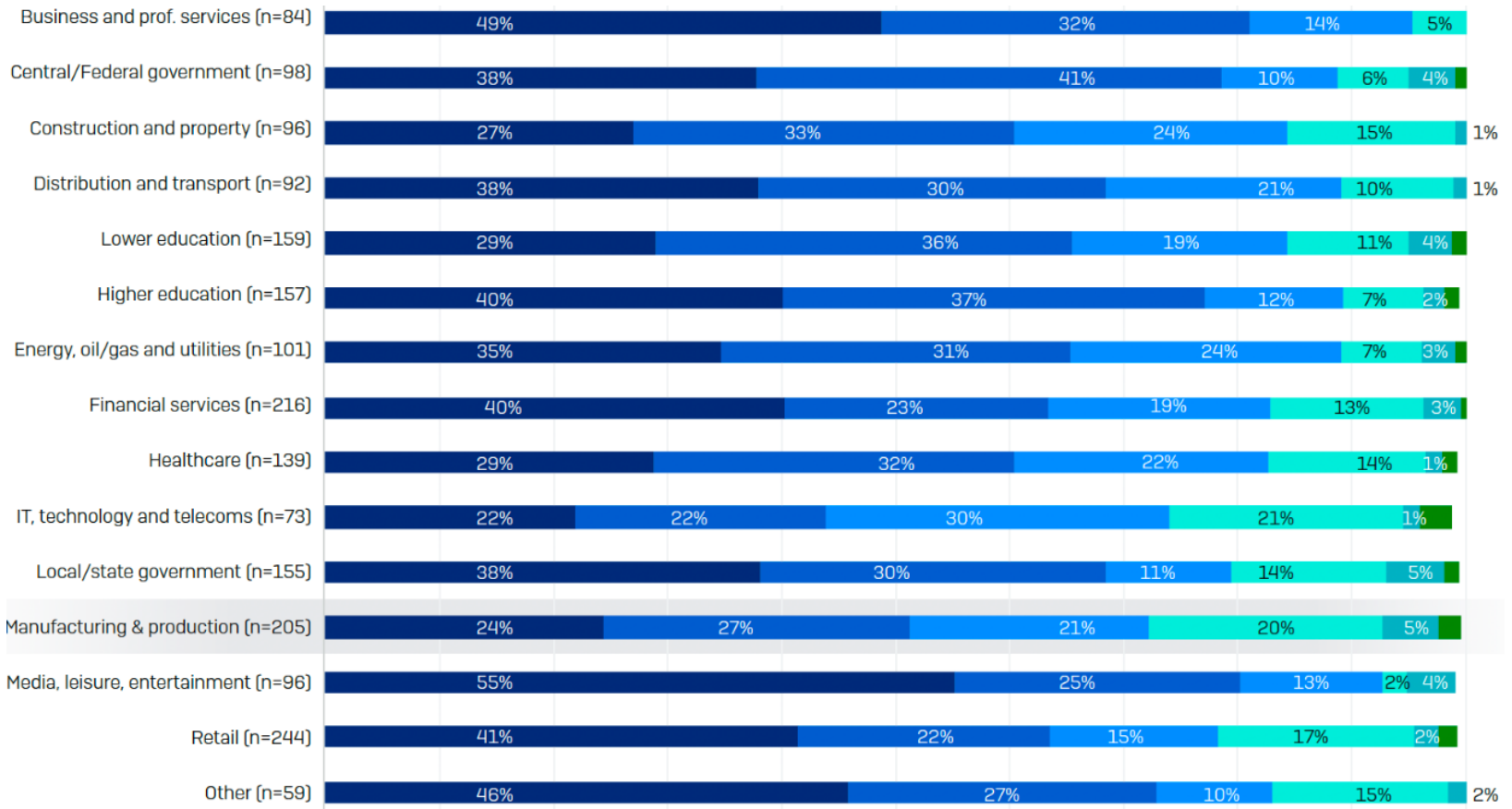
Ransom Payments by Manufacturing and Production: 2023 vs. 2022



How much was the ransom payment that was paid to the attackers? Excluding 'Don't know' responses. n=25 (2023)/ 38 (2022).
Manufacturing has low base numbers, so the findings should be considered indicative.

Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

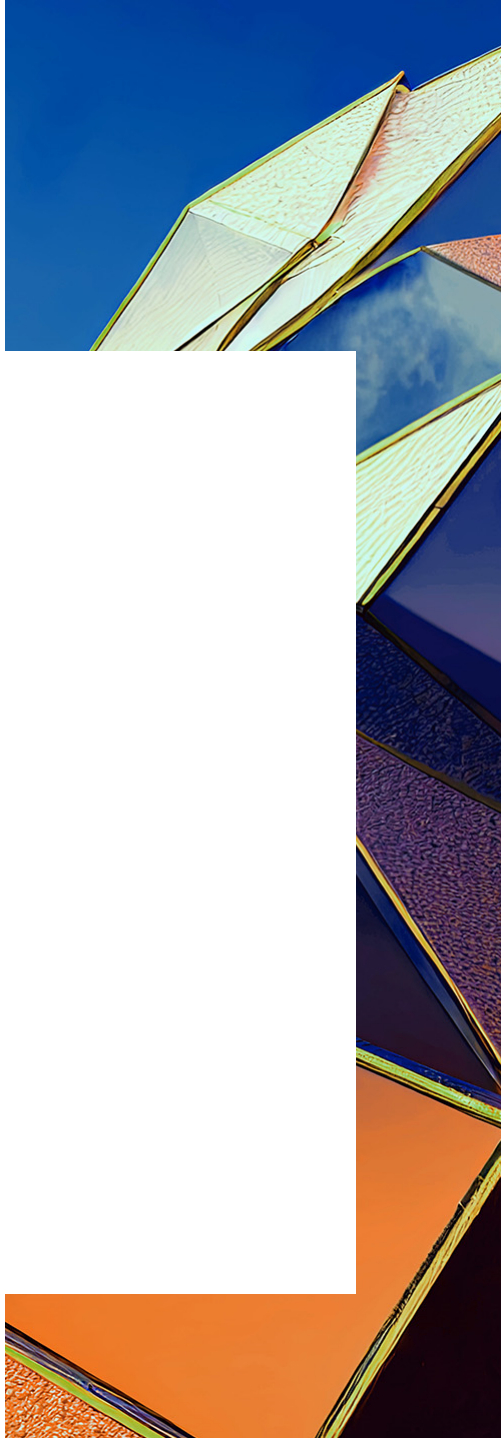
Root Cause of Attack by Industry

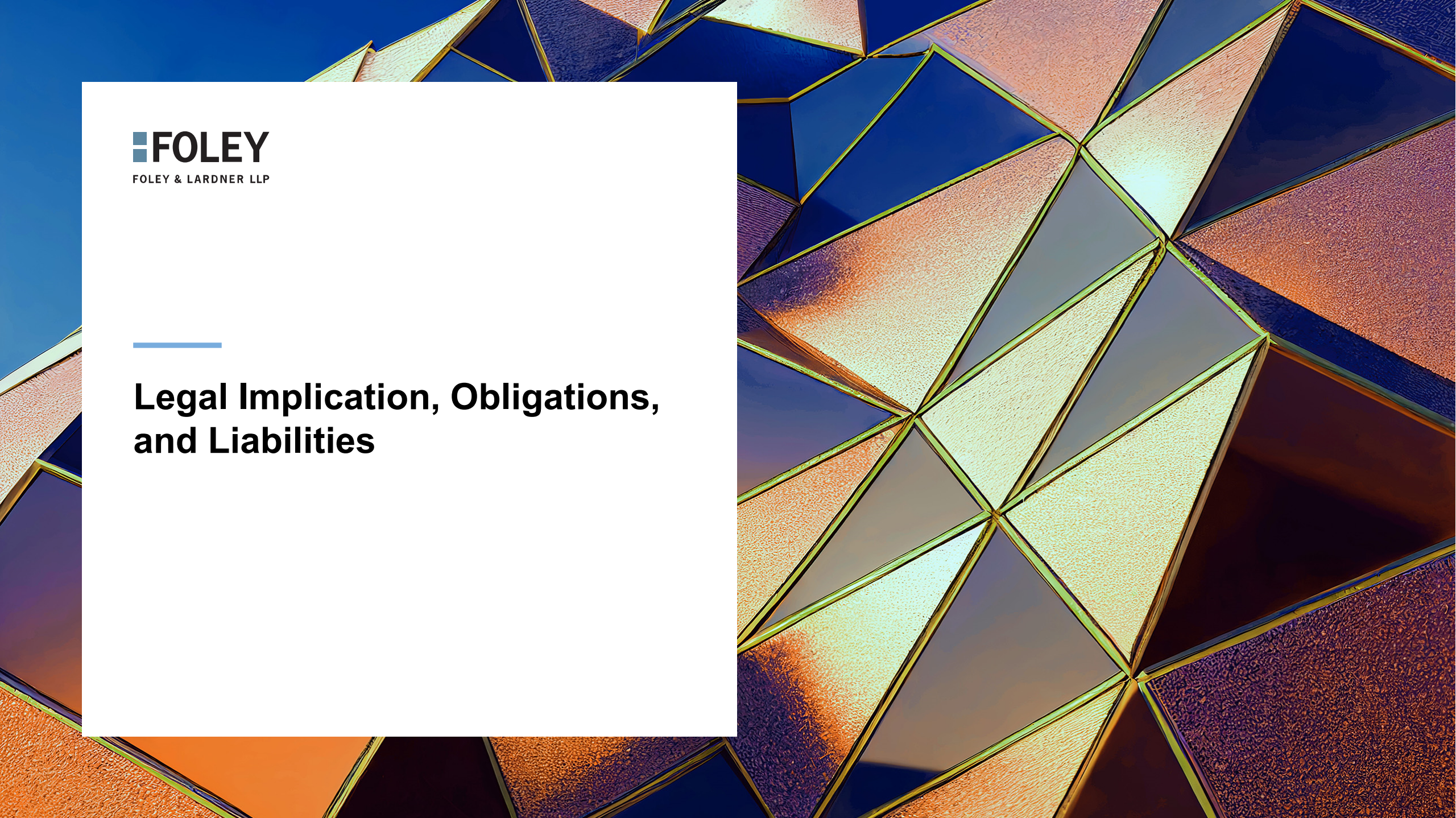


Source: The State of Ransomware in Manufacturing and Production 2023, A Sophos Whitepaper. June 2023

Navigating the Complex Terrain of Cybersecurity Challenges Today

- A Shortage of Skilled Cybersecurity Professionals
- Supply Chain Vulnerabilities
- Bridging the IT-OT/ICS Gap
- Constantly Evolving Cyber Threat Landscape
- The Proliferation of Industrial Internet of Things (IIoT)
- Increased Sophistication and Funding of Adversaries





FOLEY

FOLEY & LARDNER LLP

Legal Implication, Obligations, and Liabilities

FOLEY

FOLEY & LARDNER LLP

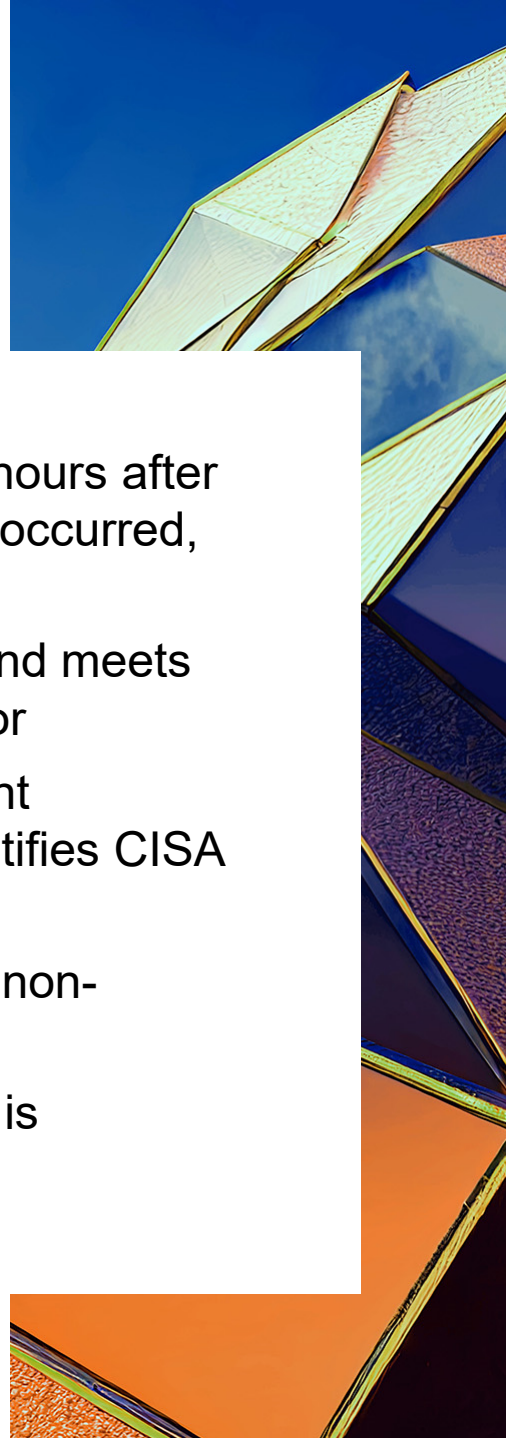
Current Legislation and Legal Obligations

FOLEY.COM

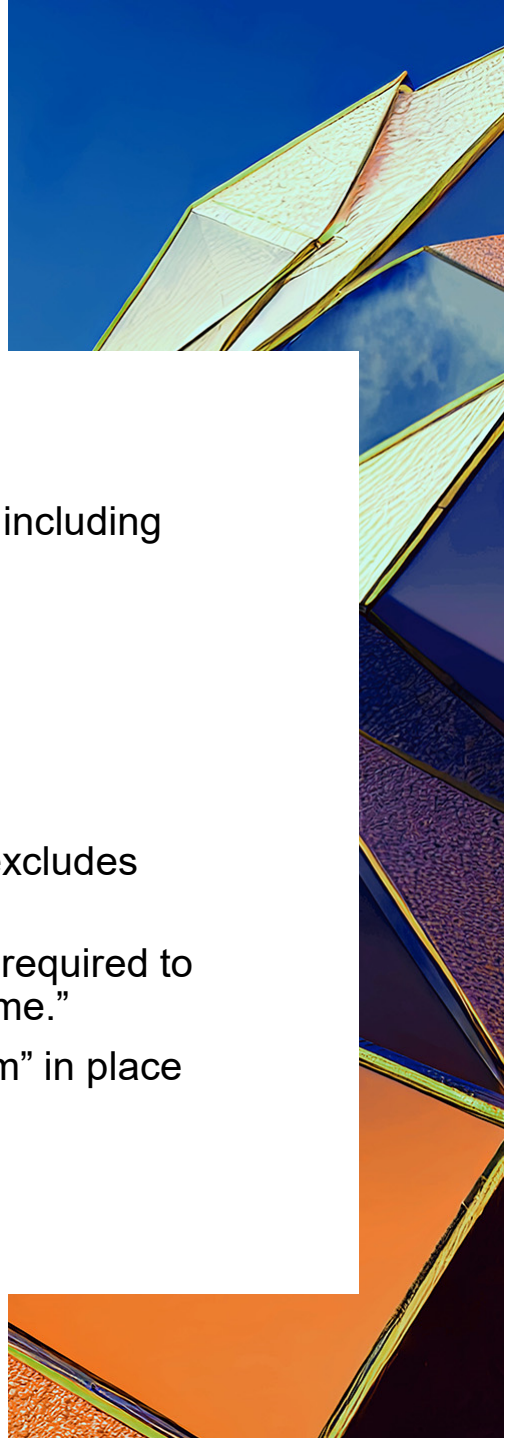
The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018

- Rapid Deployment
- Incident Analysis
- Threat Intelligence Sharing

- Report certain covered cyber incidents to CISA within 72 hours after the entity "reasonably believes" that such an incident has occurred, and ransomware payments within 24 hours
  - A "covered cyber incident" as one that is "substantial" and meets the "definition and criteria" to be set by the CISA Director
- Required to submit updates as "substantial new or different information becomes available" until the covered entity notifies CISA that the incident has been fully mitigated and resolved.
- Voluntary reporting of incidents and ransom payments by non-covered entities
- Voluntary provision of additional information beyond what is mandatory by covered entities

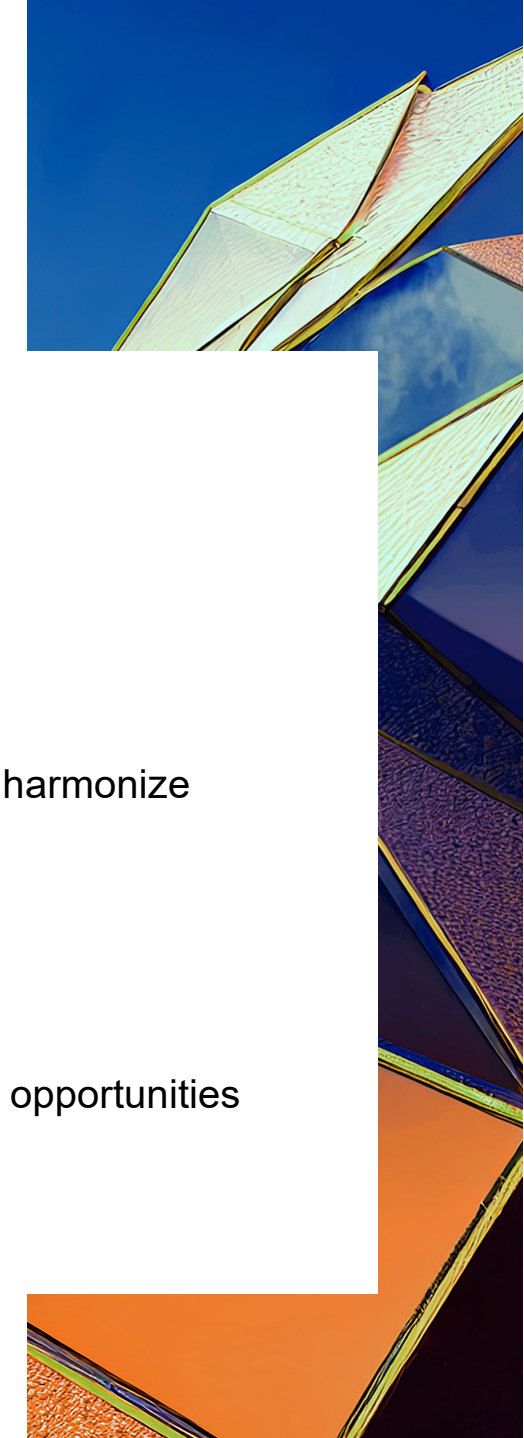


Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)



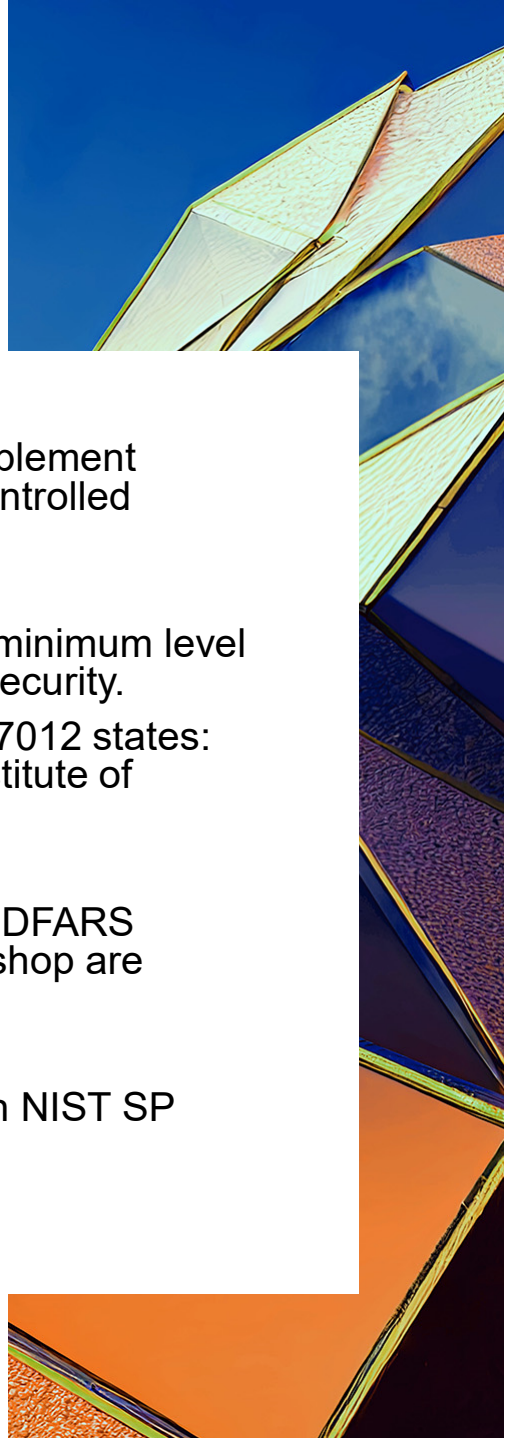
- Required and voluntary reporting will receive certain protections
  - Reports cannot be used by CISA, other federal agencies, or any state or local government to regulate, including through enforcement action, the activities of the covered entity that submitted the report;
  - Considered commercial, financial, and proprietary information if so designated;
  - Exempt from disclosure under freedom of information laws and similar disclosure laws;
  - Do not constitute a waiver of any applicable privilege or protection provided by law; and
  - Are not subject to a federal rule or judicial doctrine regarding *ex parte* communications
  - No cause of action based on the report (does not prevent litigation based on underlying incident), but excludes actions to enforce subpoena by federal government
  - But excludes reporting requirements covered entities that, "by law, regulation, or contract," are already required to report "substantially similar information to another Federal agency within a substantially similar timeframe."
    - Only available only if the relevant federal agency has an "agency agreement and sharing mechanism" in place with CISA
  - Reports to be available to Sector Risk Management Agencies and federal agencies within 24 hours

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)



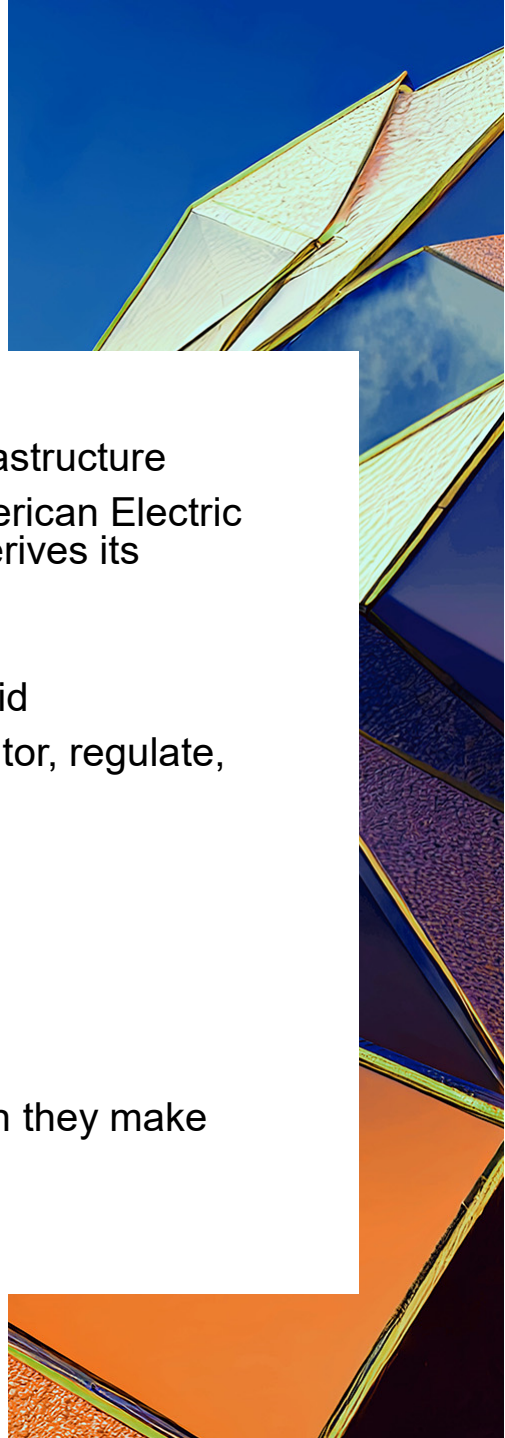
- Failure to submit a required report
  - CISA Director may issue a subpoena
  - Referral of the matter to the Department of Justice
  - Denied covered entities some of the protections for failure to comply
- Up Next
  - Cyber Incident Reporting Council
    - DHS to lead an intergovernmental Cyber Incident Reporting Council to “coordinate, deconflict, and harmonize Federal incident reporting requirements”
  - Ransomware Vulnerability Warning Pilot Program
    - Identify the most common security vulnerabilities in ransomware attacks
    - How to defend, mitigate, and contain the security vulnerabilities
  - Joint Ransomware Task Force
    - “coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.”

Defense Federal Acquisition Regulation Supplement (DFARS)



- All Department of Defense (DoD) contractors must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum cybersecurity standards or risk losing federal contracts. This includes safeguarding controlled unclassified information (CUI) and complying with the NIST Special Publication 800-171 standards.
- NIST 800-171
  - Cybersecurity standard rather than a regulatory requirement, but commonly understood to establish a minimum level of good cybersecurity practice/guidance akin to a requirement to meet DFARS requirements for cybersecurity.
  - DFARS is a DoD publication that sets the rules for participating in defense contracts. DFARS 252.204-7012 states: “the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171”
- Cybersecurity Maturity Model Certification (CMMC)
  - Unified cybersecurity standard that adds a verification component to the cybersecurity requirements in DFARS 252.204-7012. Establishes different levels so that the cybersecurity requirements for a small machine shop are simpler and easier to meet than those for a Tier 1 original equipment manufacturer (OEM).
  - All DoD contracts to ensure CMMC compliance by October 21, 2025
  - To be eligible for DoD contracts, a contractor must complete a self-assessment of their compliance with NIST SP 800-171
- Failure to meet these requirements can result in contract termination and legal consequences.

Federal Energy Regulatory Commission (FERC)



- FERC establishes cybersecurity standards for the energy sector to protect the nation's critical energy infrastructure
  - Cybersecurity standards for the bulk power system in the United States are governed by the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards (NERC derives its authority from FERC)
  - Covers United States, Canada, and parts of Mexico
  - Failure to comply can result in penalties, loss of licenses, and damage to the reliability of the energy grid
- Framework of 14 ratified and proposed standards that outline recommended controls and policies to monitor, regulate, manage and maintain the security of critical infrastructure systems
  - CIP-003-9 Cyber Security – Security Management Controls.
  - CIP-004-6 Cyber Security -- Personnel and Training.
  - CIP-008-6 Cyber Security -- Incident Reporting and Response Planning.
  - CIP-013-1 Cyber Security -- Supply Chain Risk Management.
  - CIP-014-1 Physical Security.
- New voluntary cyber incentive framework allow utilities to apply for an incentive-based rate recovery when they make certain pre-qualified cybersecurity investments or join a threat information-sharing program

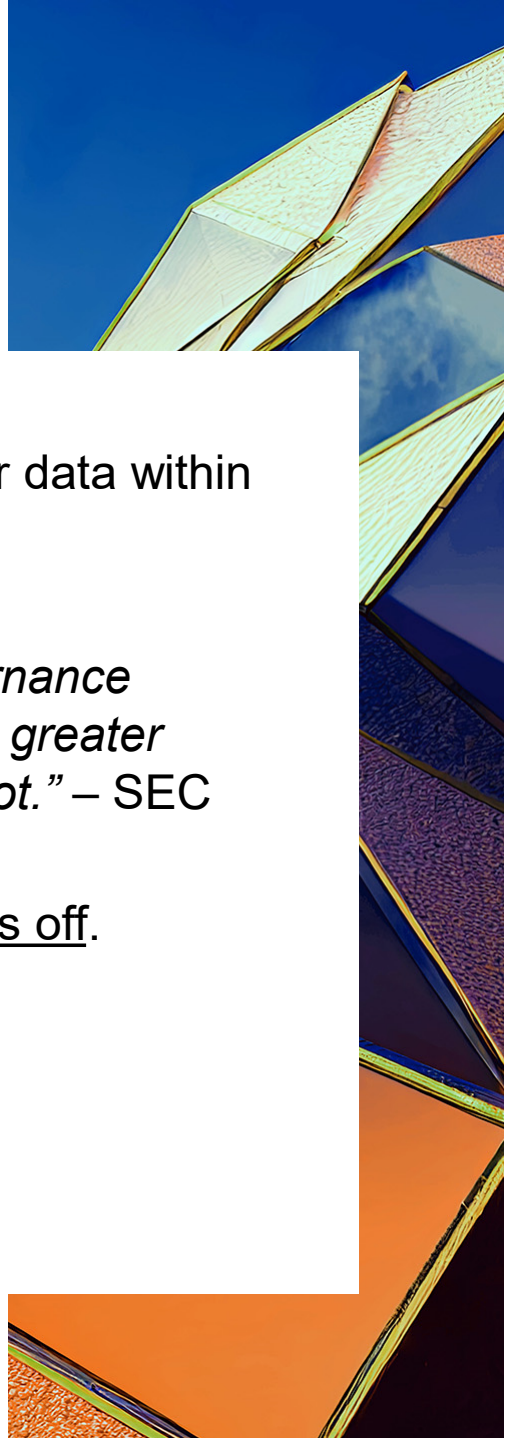
FOLEY

FOLEY & LARDNER LLP

The U.S. Securities and Exchange Commission (SEC)

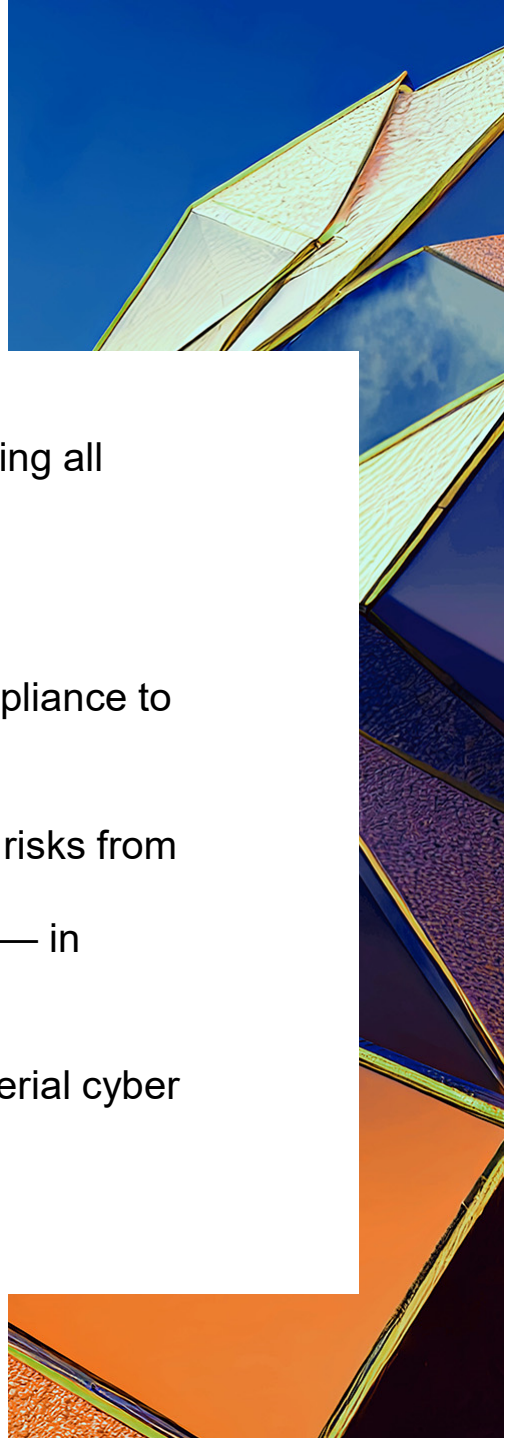
FOLEY.COM

Understanding the New SEC Cybersecurity Rules



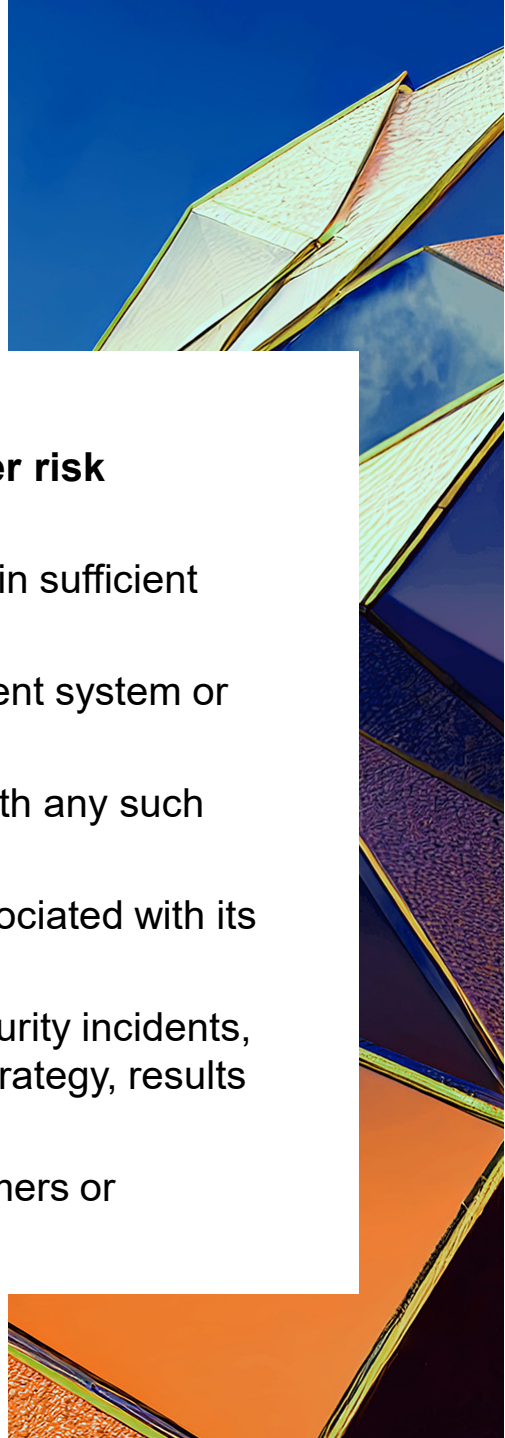
- …they're calling your bluff. Be transparent about how you protect your systems and your data within them…with a focus on the interests of an informed, "reasonable investor."
- Any kind of cyber-related incident matters. This is not another "data breach" regulation.
- *"To the extent investors view strong cybersecurity risk management, strategy, and governance favorably, registrants disclosing more robust processes, more clearly, could benefit from greater interest from investors, leading to higher market liquidity relative to companies that do not."* – SEC Cybersecurity Risk Management Final Rule
- The SEC is creating a market condition where long-term planning and transparency pays off.

Final SEC Cybersecurity Disclosure Rules: Overview



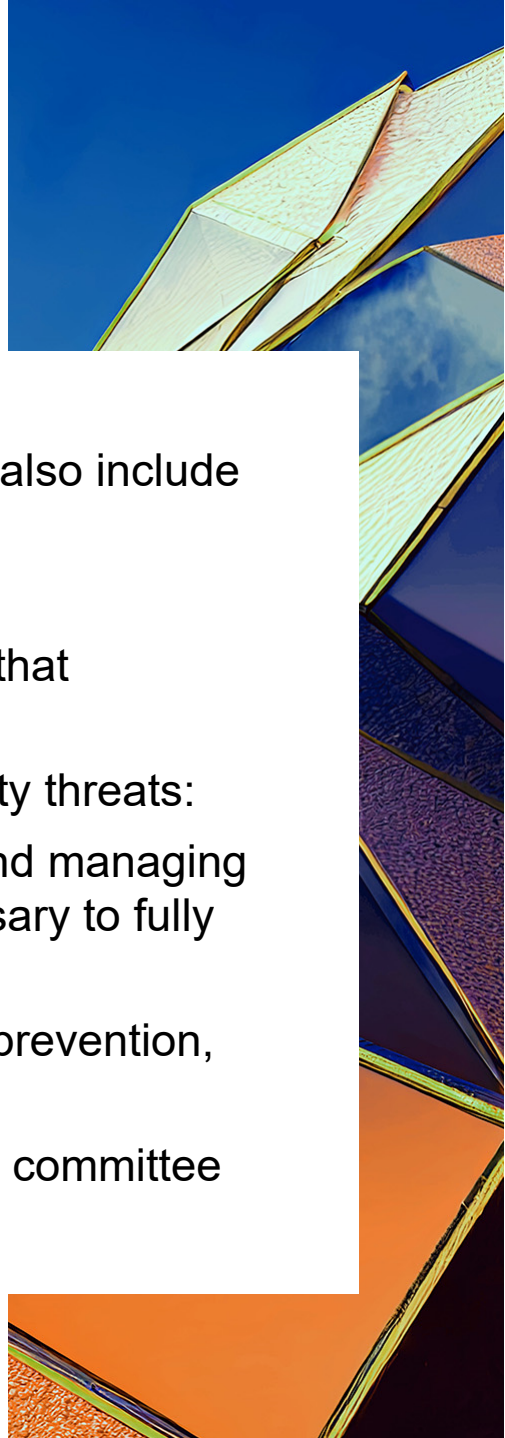
- Additional disclosure requirements for U.S. reporting companies, as well as foreign private issuers, including all companies with stock traded on U.S. stock exchanges (together, “public companies”)
- The final rule was effective on September 15, 2023, with compliance dates of:
  - Form 10-K disclosure: For all companies for the fiscal year ending on or after **December 15, 2023**, in upcoming annual reports
  - Incident reporting on Form 8-K: Beginning on December 18, 2023 (with an additional 180 days for compliance to June 15, 2024, for smaller reporting companies)
- Annually on Form 10-K:
  - Describe a company’s **risk management** processes for assessing, identifying, and managing material risks from cybersecurity threats
  - Discuss the **governance framework** — including the Board’s oversight role, and management’s roles — in assessing and managing material cybersecurity risk
- Current/incident reporting on Form 8-K:
  - Public reporting of material incidents within four business days of a determination that there was a material cyber incident occurring on a company’s IT system
  - Disclosure of any material updates on an ongoing basis

SEC Annual Reporting on Form 10-K: Disclosure Items



- In each Form 10-K, filed publicly via the SEC's EDGAR system, a public company must now include **cyber risk management** disclosures
- Description of processes for assessing, identifying, and managing material risks for cybersecurity threats in sufficient detail for a reasonable investor to understand, such as:
  - Whether and how any such processes have been integrated into the company's overall risk management system or processes;
  - Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
  - Whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider
- Explanation of whether (and, if so, how) any risks from cybersecurity threats, including previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition
  - SEC provides examples of risks, including disruption to business operations, theft of IP, harm to customers or employees, reputational harm, legal risks

SEC Annual Reporting on Form 10-K: Disclosure Items (cont'd.)

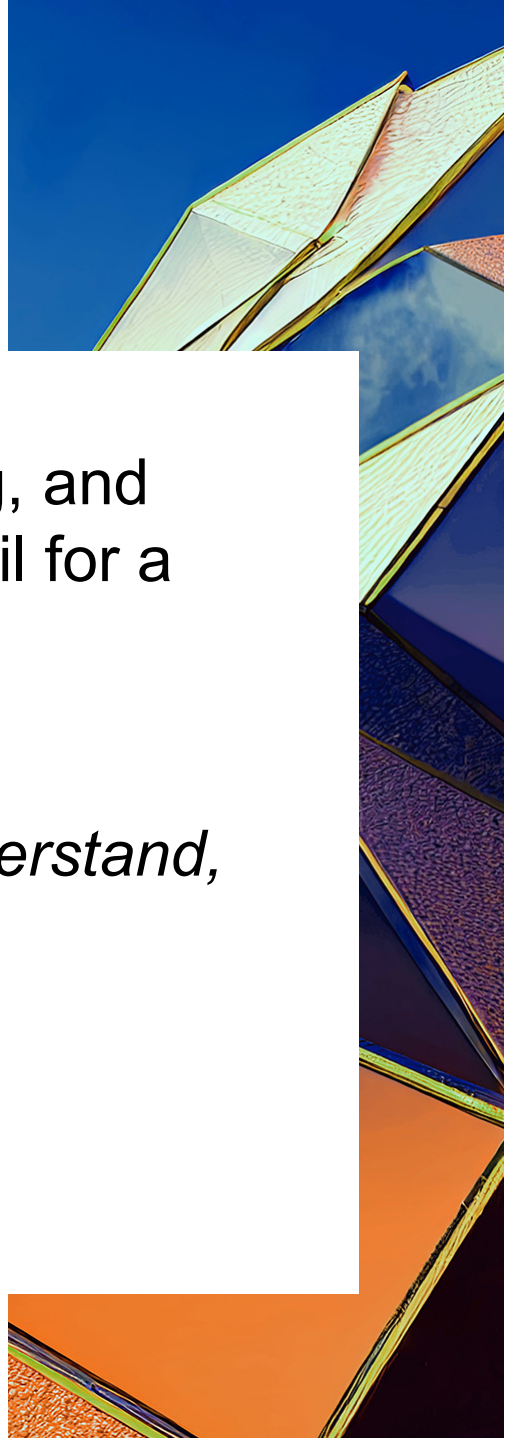


- In each Form 10-K, filed publicly via the SEC's EDGAR system, a public company must now also include **cyber governance** disclosures
- The Board's oversight of risks from cybersecurity threats
  - What Board committee, if any, is responsible for cyber risk oversight; a description of how that committee is informed of risks
- Management's role in assessing and managing the company's material risk from cybersecurity threats:
  - Whether and which management positions or committees are responsible for assessing and managing such risks and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
  - The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
  - Whether such persons or committees report information about such risks to the Board or a committee or subcommittee of the Board

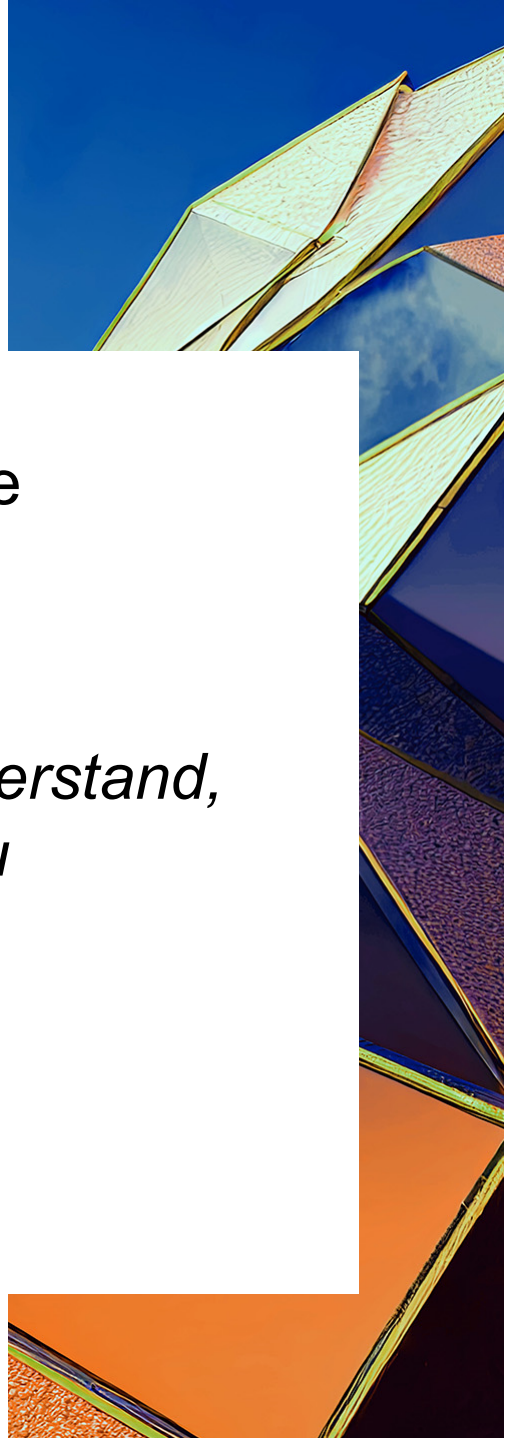
Form 10-K Disclosure Requirement: Processes

Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes

The market sees this: *"Please tell investors, in a way they will understand, how you manage the cybersecurity risks that may hurt them."*



Form 10-K Disclosure Requirement: Processes (cont'd.)



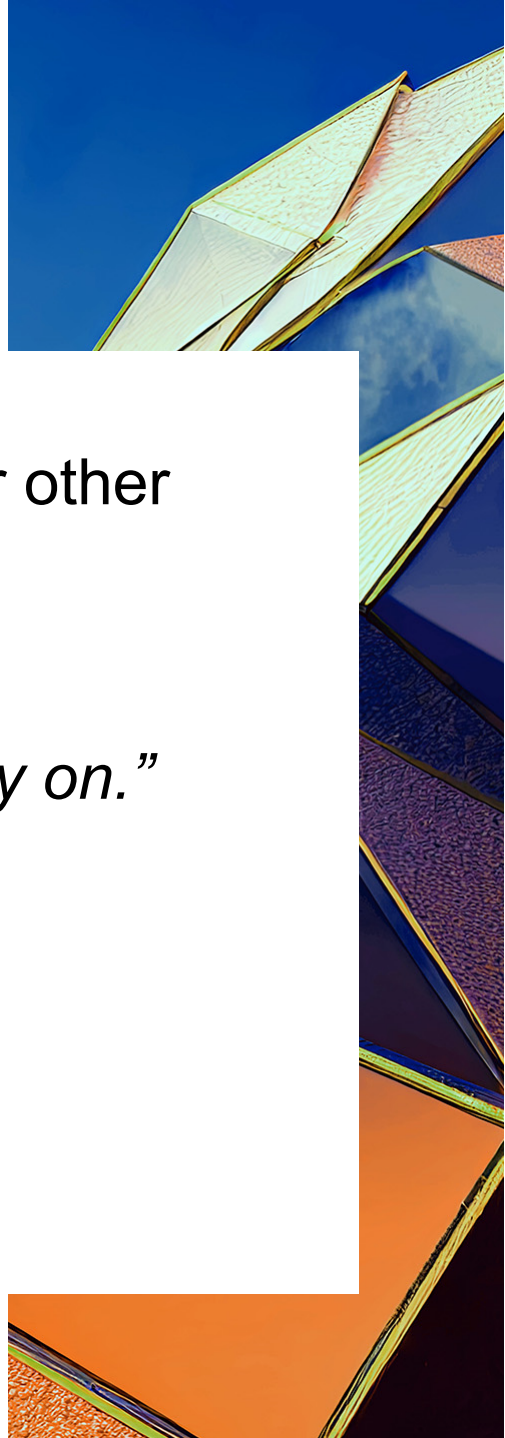
Whether and how any such processes have been integrated into the registrant's overall risk management system or processes

The market sees this: *"Please tell investors, in a way they will understand, how you make cybersecurity risk as important as the other risks you manage."*

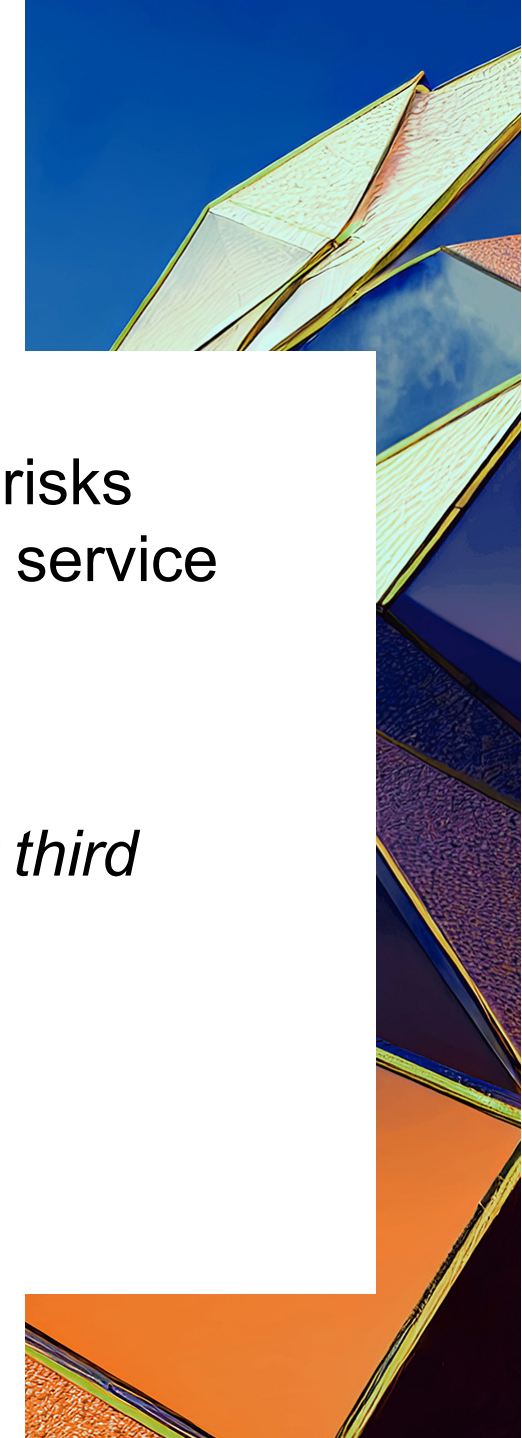
Form 10-K Disclosure Requirement: Processes (cont'd.)

Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes

The market sees this: *"Please tell investors what expertise you rely on."*



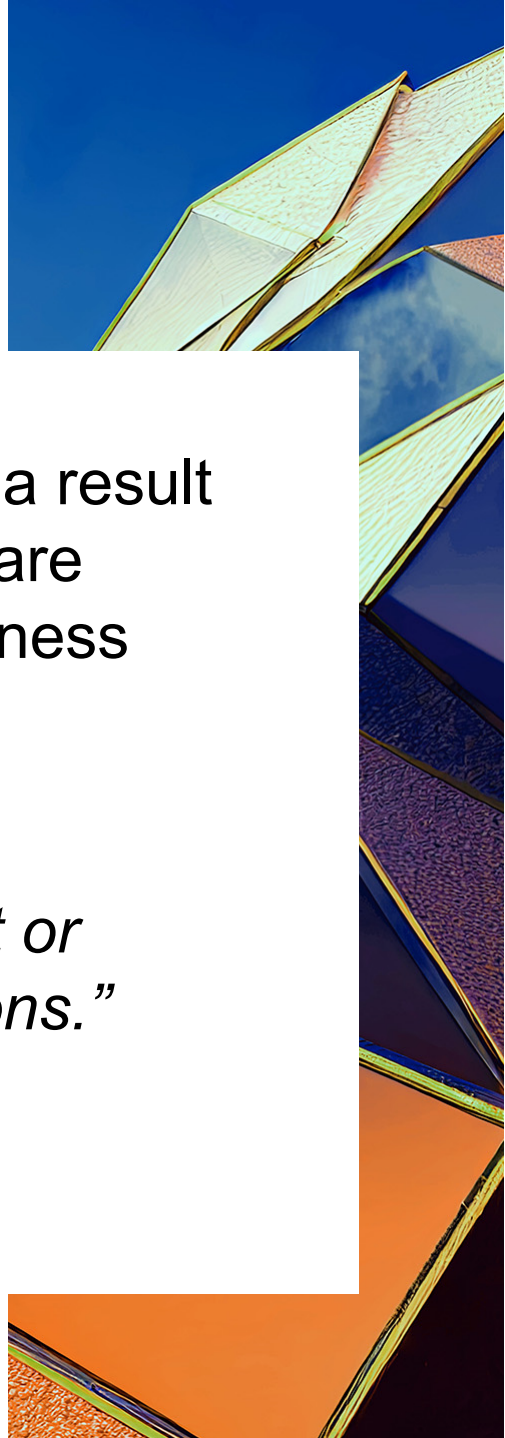
Form 10-K Disclosure Requirement: Processes (cont'd.)



Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider

The market sees this: *"Please tell investors whether you consider third parties who pose risks to you as a risk to your investors."*

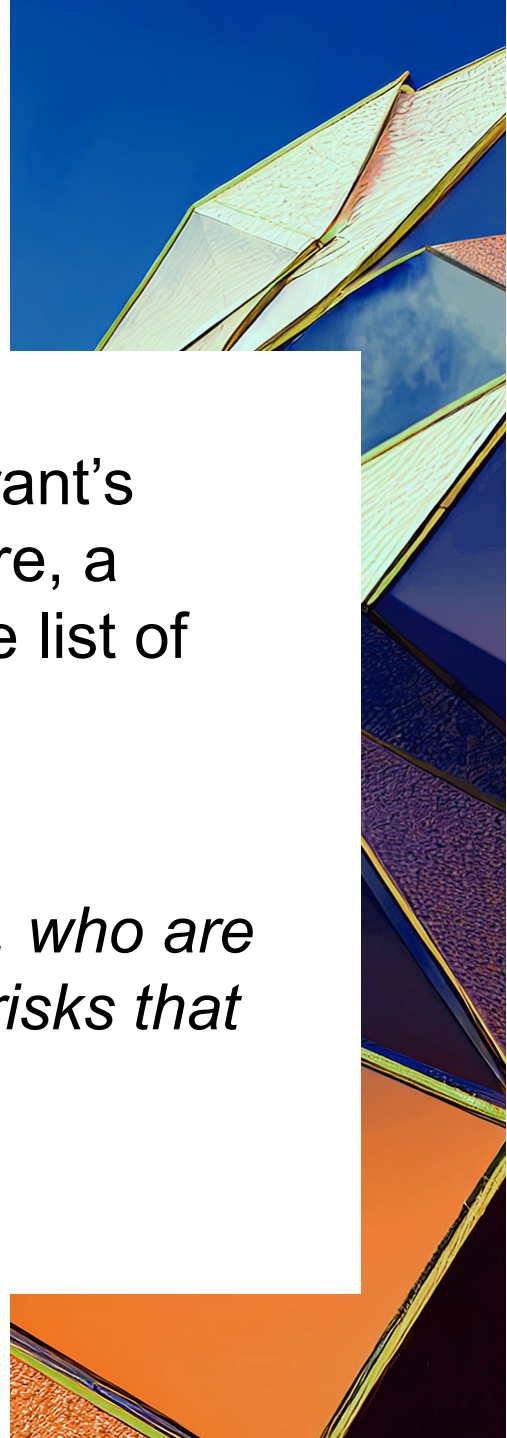
Form 10-K Disclosure Requirement: Risks



Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how

The market sees this: *“Please tell investors about how any current or previous incidents should inform their voting and investment decisions.”*

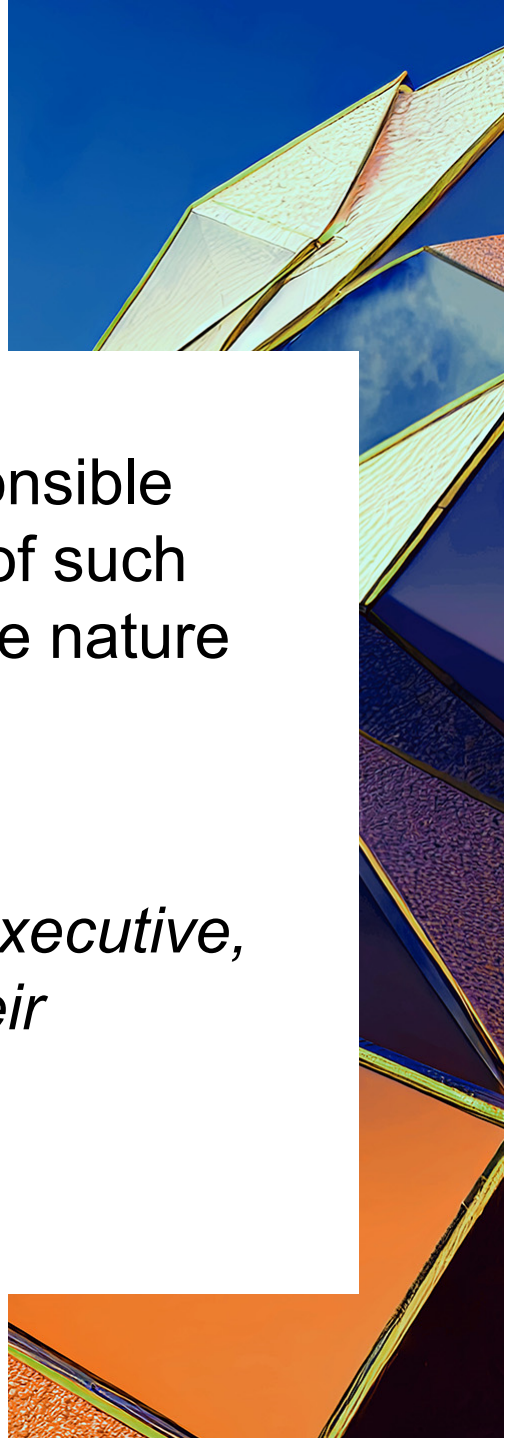
Form 10-K Disclosure Requirement: Risks (cont'd.)



Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

The market sees this: *"Please tell investors whether management, who are responsible for running the company, are involved in cybersecurity risks that pose a risk of harm to investors."*

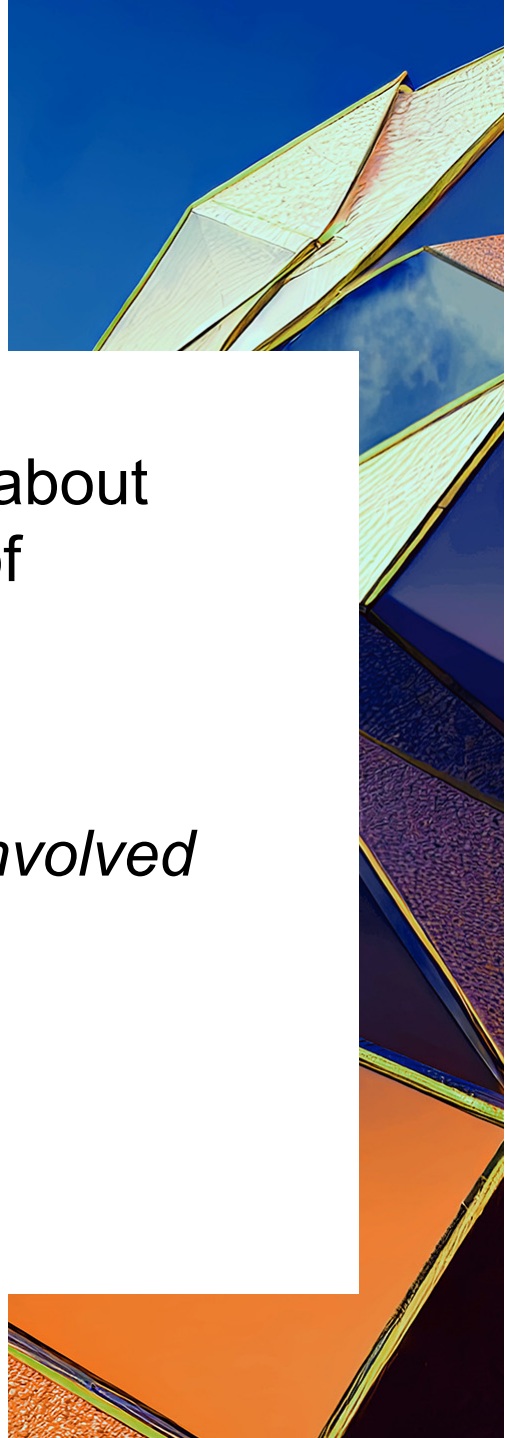
Form 10-K Disclosure Requirement: Governance



Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise

The market sees this: *“Please tell investors which management, executive, or director positions are involved in cybersecurity risks and what their expertise is.”*

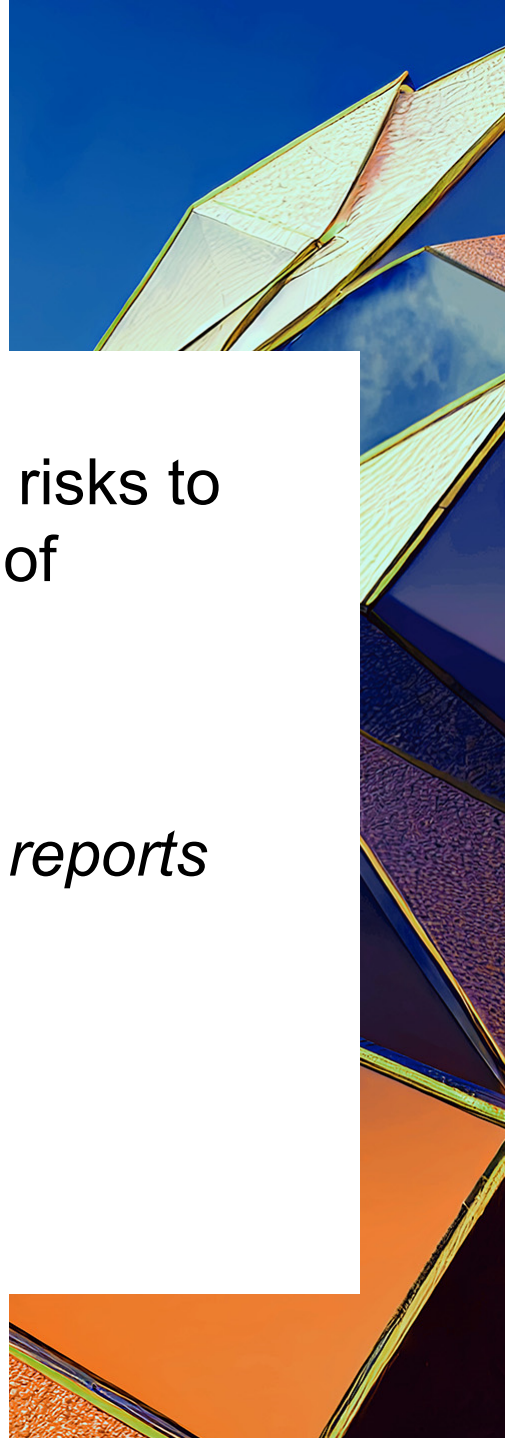
Form 10-K Disclosure Requirement: Governance (cont'd.)



The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents

The market sees this: *"Please tell investors how management is involved in cybersecurity incident management."*

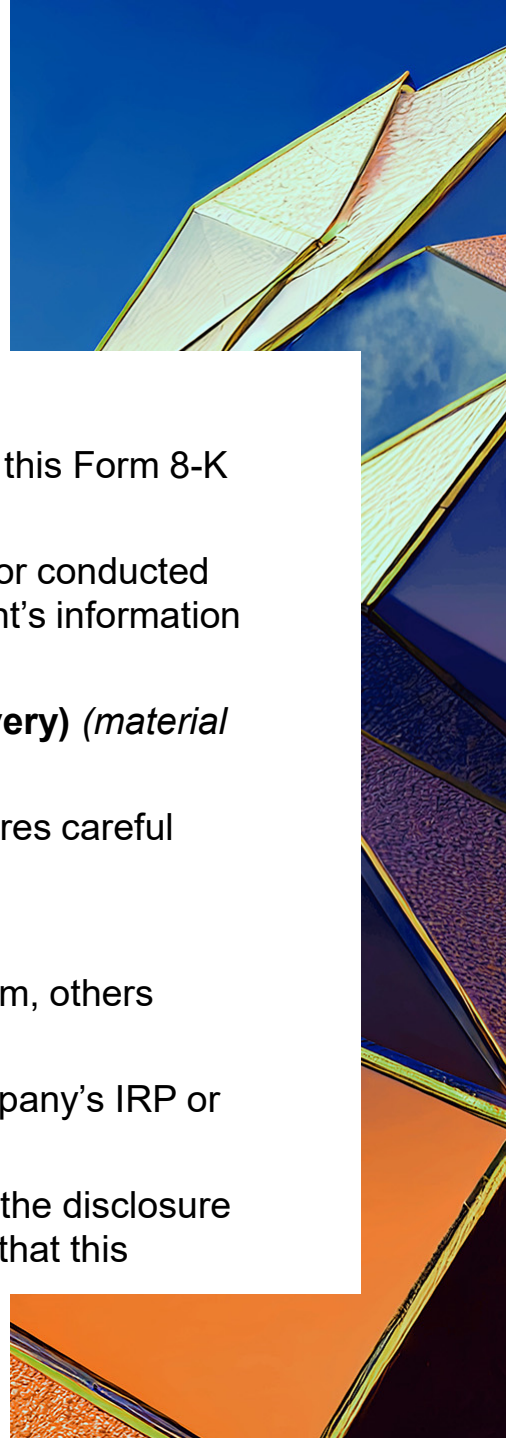
Form 10-K Disclosure Requirement: Governance (cont'd.)



Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors

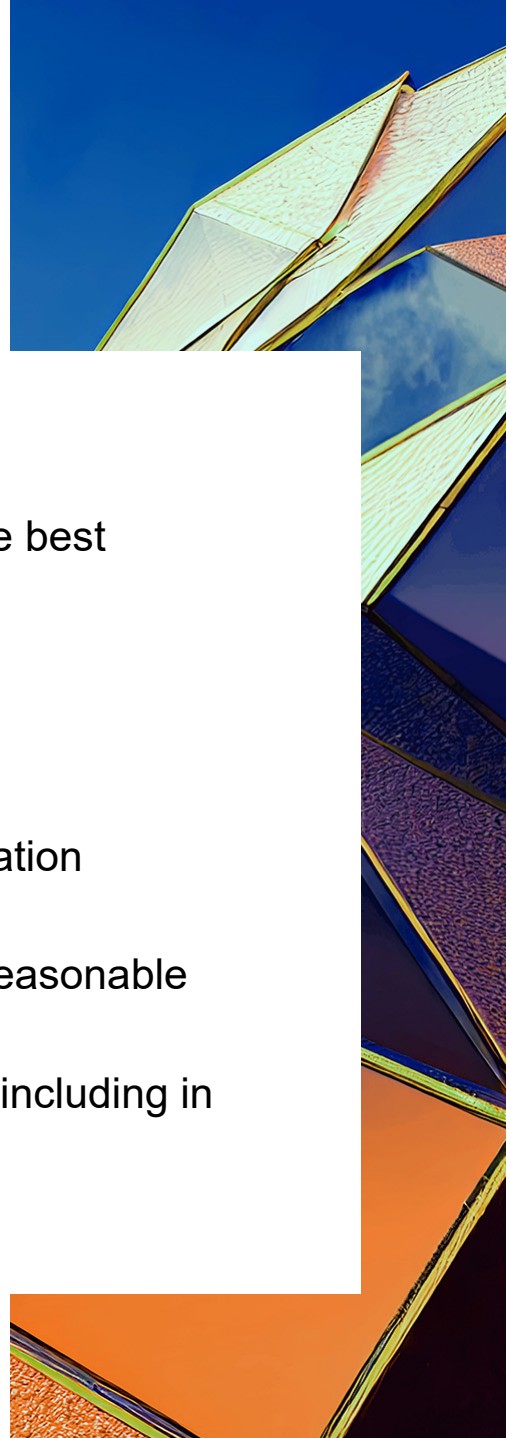
The market sees this: *"Please tell investors whether management reports incidents to investors."*

SEC Material Event Reporting on Form 8-K: Required Disclosure of Material Cybersecurity Incidents



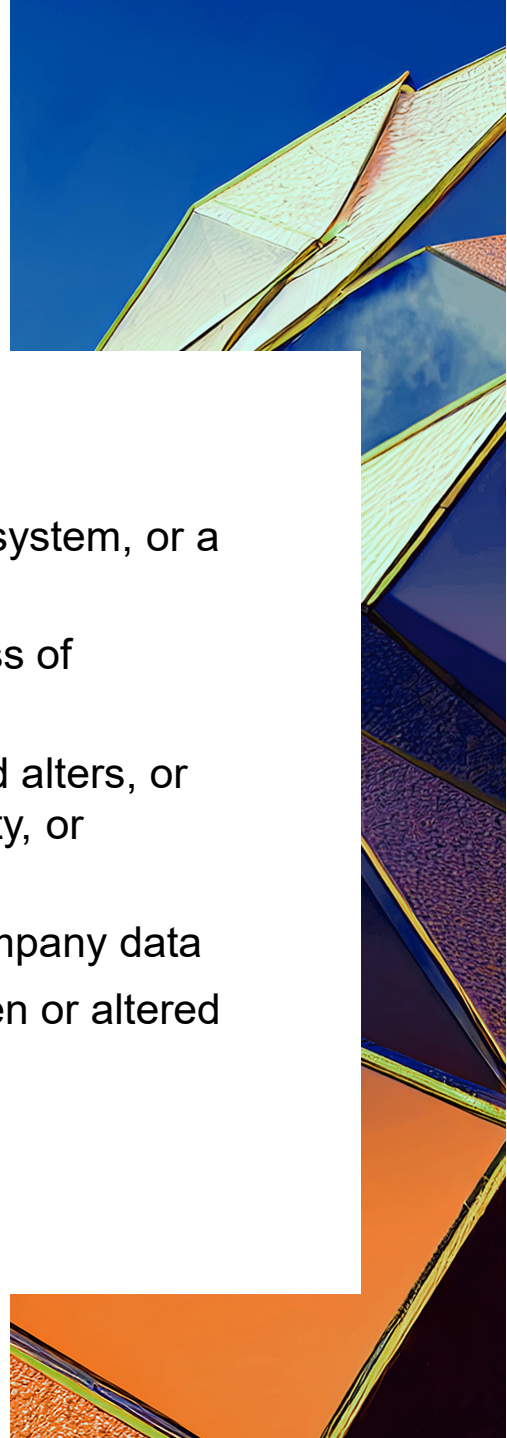
- The SEC's rule established a new item 1.05 to Form 8-K requiring disclosure of a material cybersecurity incident; this Form 8-K filing is made via the SEC's EDGAR system and is publicly available to all
- "Cybersecurity incident" means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein
- Reporting is **required within four business days** of a determination of **materiality (<u>not</u> date of incident discovery)** *(material updates to be made on subsequent Form 8-K amendments)*
  - Determination of materiality may not occur for a substantial period of time after an incident is discovered; requires careful documentation of process
  - Important to be diligent in evaluating incidents to make materiality determinations without unreasonable delay
    - Appropriate personnel at company must be involved: legal, CISO, disclosure committee, Board, finance team, others involved with IRP
  - May be necessary to re-evaluate materiality if an incident is re-classified to a higher classification under a company's IRP or significant new facts become known
  - Rule allows a company to delay disclosure for up to 30 days if the U.S. Attorney General notifies the SEC that the disclosure would pose a substantial risk to national security or public safety; will be in only "extraordinary circumstances" that this exemption will arise

When is an Incident “Material” for Purposes of Form 8-K Reporting?



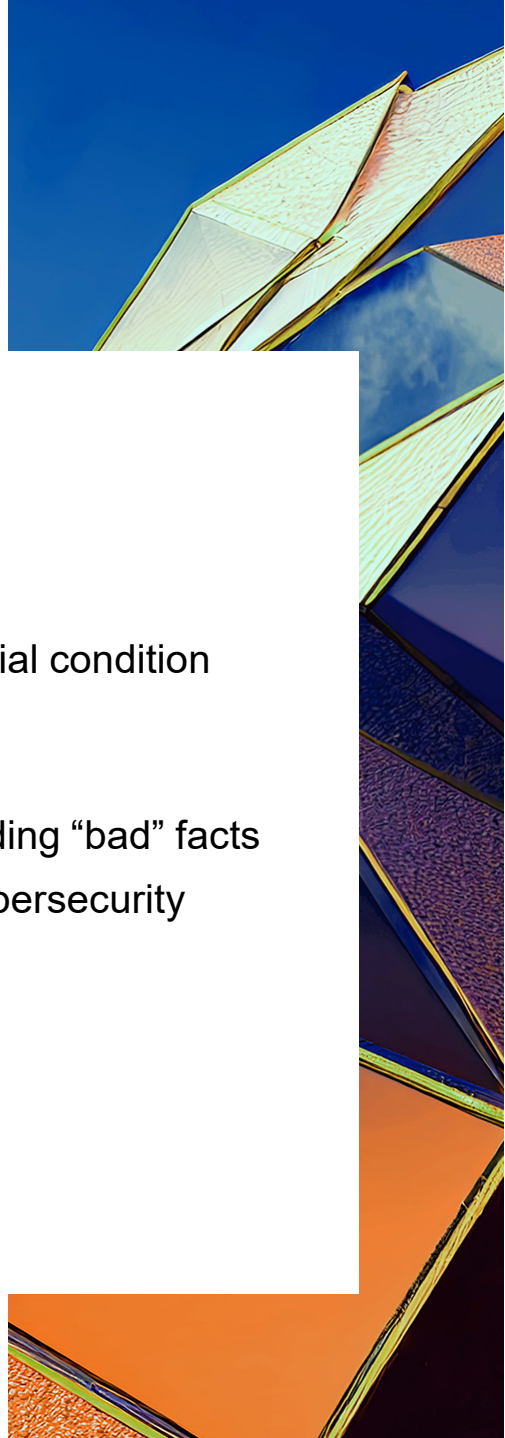
- Materiality is a legal determination based on the "facts and circumstances" of the matter
- The SEC has declined to identify what it believes to be material, stating that each company is in the best position to know what is material to its own investors
  - Factors to be considered include:
    - The nature, extent, and potential magnitude of the risk/incident
    - The range of potential harms to various stakeholders
    - Whether there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision
    - If not disclosed, whether disclosure of the omitted information would have been viewed by a reasonable investor as having significantly altered the total mix of information available
  - Consider intersection with other materiality determinations made for financial reporting reasons, including in periodic reporting and financial statement footnotes, though other contexts not determinative

When is an Incident "Material" for Purposes of Form 8-K Reporting? (cont'd.)



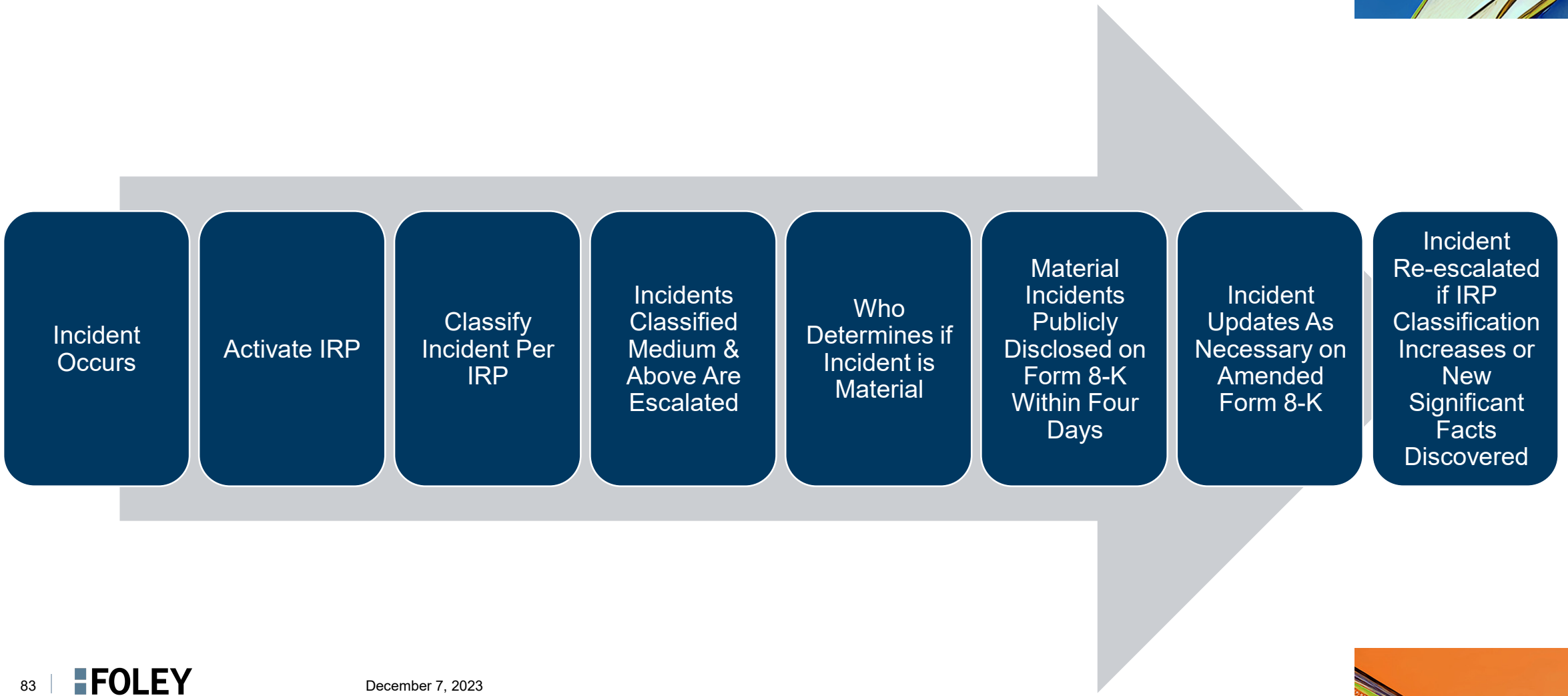
- **Examples from the SEC's final release of incidents that may be material include:**
  - An unauthorized incident that compromises the confidentiality, integrity, or availability of data, a system, or a network, or violates the company's security policies or procedures
  - An unauthorized incident that causes degradation, interruption, loss of control, damage to, or loss of operational technology systems
  - An incident in which an unauthorized party accesses (or a party exceeds authorized access) and alters, or has stolen, sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the company
  - An incident in which a malicious actor offers to sell or threatens to publicly disclose sensitive company data
  - An incident in which a malicious actor demands payment to restore company data that was stolen or altered

Content of Form 8-K: Disclosure of Material Incidents

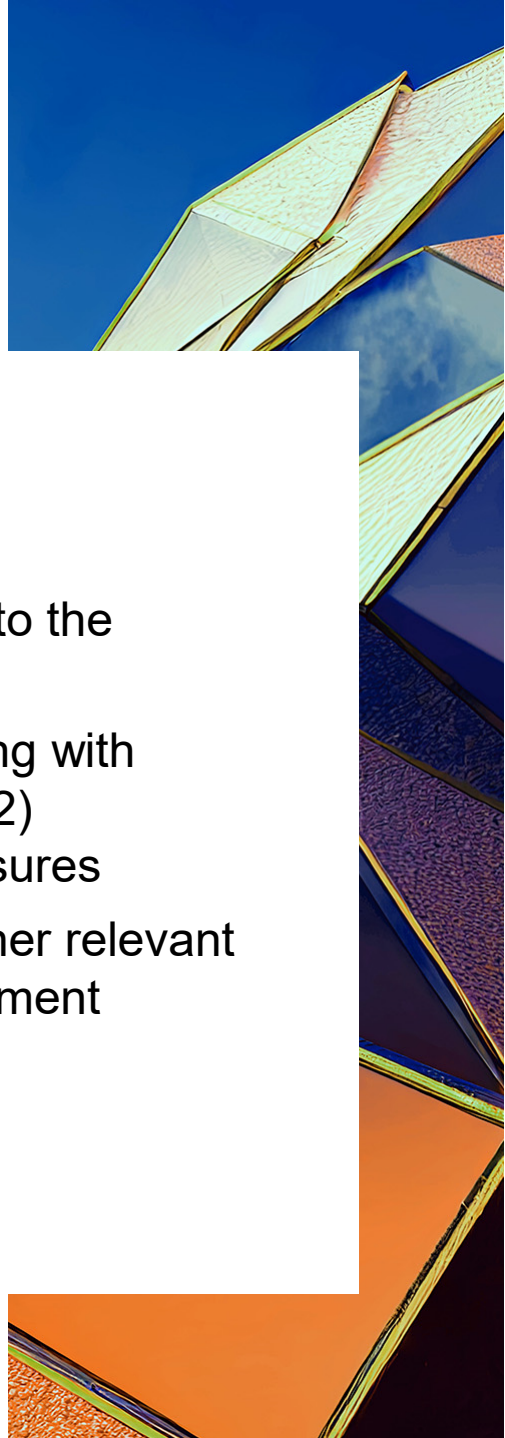


- **Disclosures should be information relevant to investors, not a road map for hackers!**
- Required disclosure content, if known, includes:
  - Material aspects of the nature, scope, and timing of the incident
  - Material impact (or reasonably likely material impact) of the incident on the company, e.g., on its financial condition and results of operations
  - Additional material information may be added as it becomes available on a Form 8-K/A
  - All disclosure must be materially accurate and complete; cannot share “good” facts and not corresponding “bad” facts
  - Do not need to disclose technical information about a planned response to the incident or impacted cybersecurity systems, related networks and devices, or potential system vulnerabilities
- Legal, CISO, financial reporting, etc., will work together to:
  - Disclose sufficient information to satisfy reporting requirements
  - Avoid disclosing information that may compromise the company’s security or remediation efforts
  - Ensure appropriate people across the organization have had the chance to review

Example: Incident Reporting Process Overview



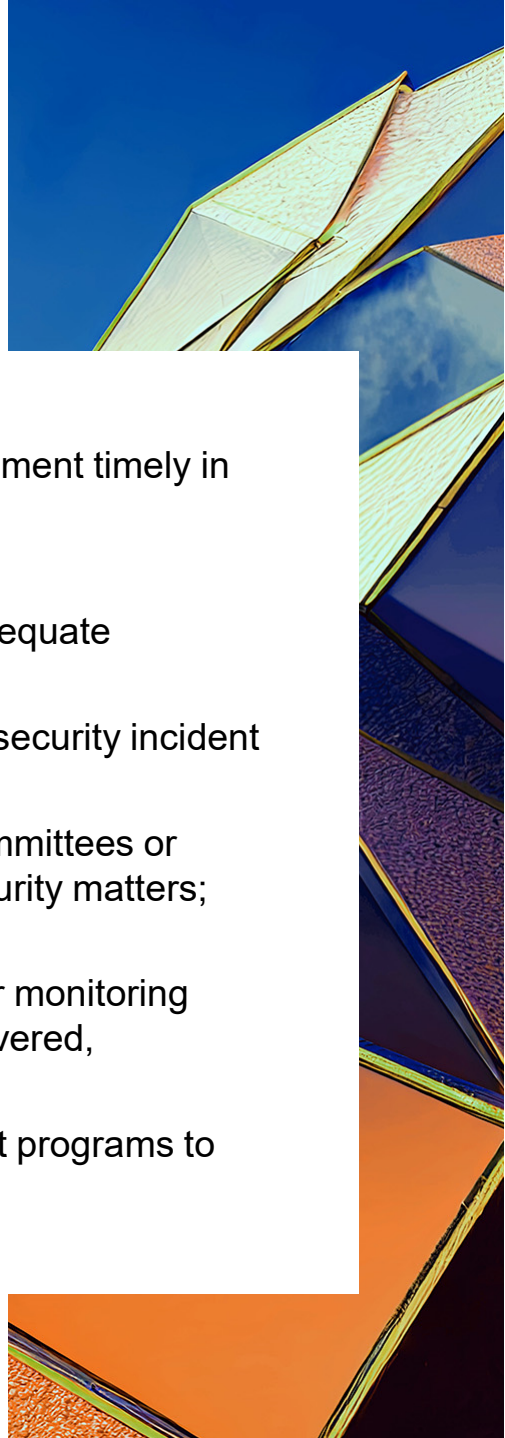
Examples of CISO Involvement in the New Disclosures



CISO involvement will be needed for:

- Accurately describing the new disclosures required in the Form 10-K
- Creating a materiality framework that may form a basis for decision-making with regard to the materiality of any future cyber incidents; prepare the framework on a “clear day”
- Assisting with (1) determining the materiality of a cyber incident to inform decision-making with regard to potential Form 8-K reporting and, once an incident is deemed to be material; (2) describing material incidents for inclusion in a Form 8-K and later, ongoing public disclosures
- Preparing a regular presentation to the Audit Committee of the Board of Directors (or other relevant committee) about potential cyber risks, cyber incidents, and the company’s risk management processes
- Advising the Board of Directors on strategies for mitigating cyber risks

Process Considerations to Support New Disclosures



- Evaluate cyber incident reporting disclosure controls and procedures to ensure information is elevated to management timely in light of the four business-day requirement to file an Item 1.05 Form 8-K
- Review and test IRPs to ensure incidents are appropriately reported throughout the organization
- IRPs should be regularly reviewed and tested, ideally through mock tabletop exercises, to ensure a timely and adequate response
- Consider delineating within the IRP or otherwise the personnel/team responsible for determining whether a cybersecurity incident is material as well as specific decision-making and documentation processes
- Boards should still be cognizant of which directors have expertise or experience with cybersecurity and which committees or subcommittees, if any, are responsible, or should be responsible, for providing oversight with respect to cybersecurity matters; amend governance documents accordingly
- To prepare for disclosure: Identify and document, if not already clear under current policies, who is responsible for monitoring risks from cybersecurity threats, how cybersecurity risks are identified, and how cybersecurity incidents are discovered, mitigated, and remedied
- There will be increased pressure for registrants to develop comprehensive, risk-based cybersecurity management programs to monitor the evolving risks to their companies

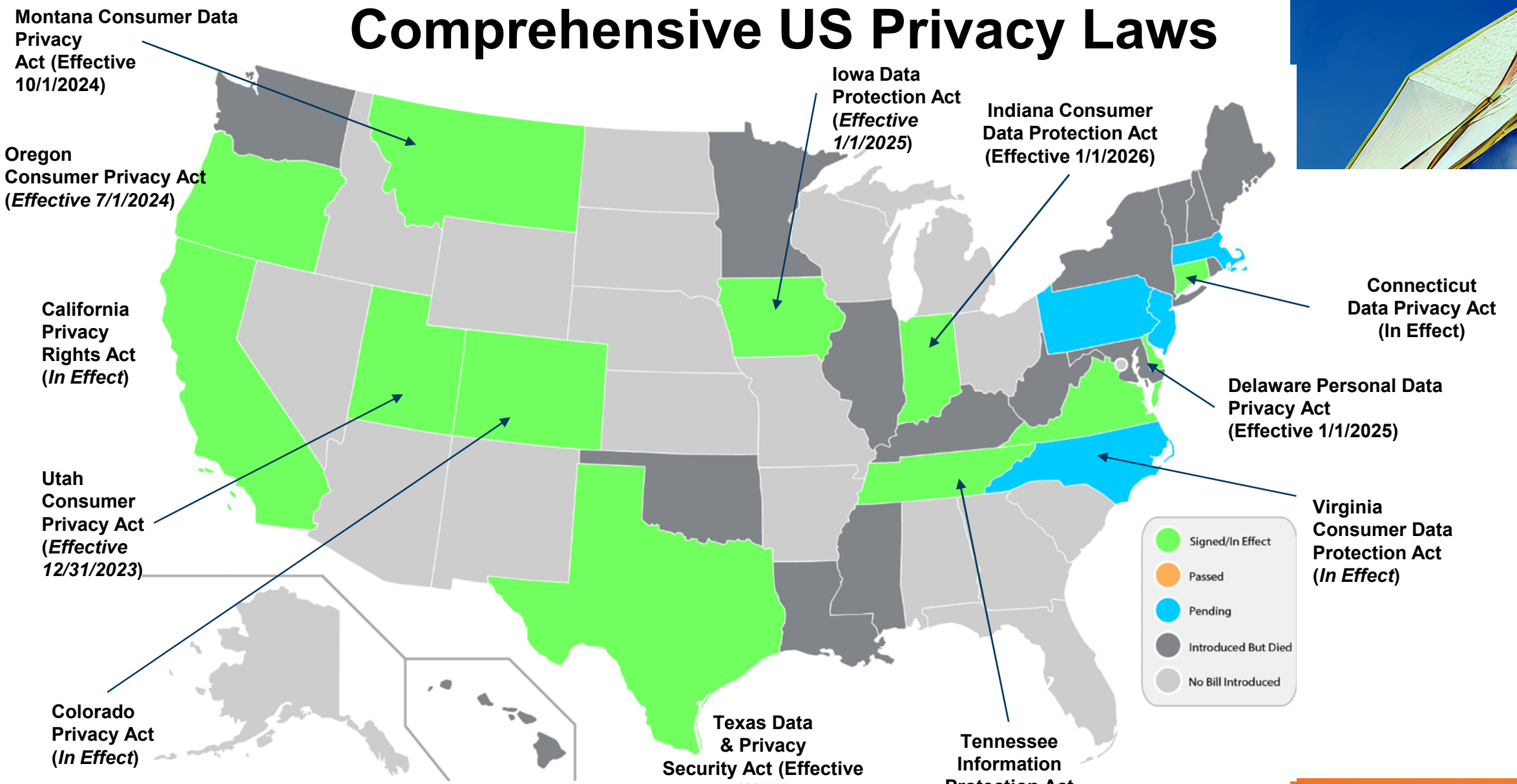
FOLEY

FOLEY & LARDNER LLP

Emerging State and Federal Legislation

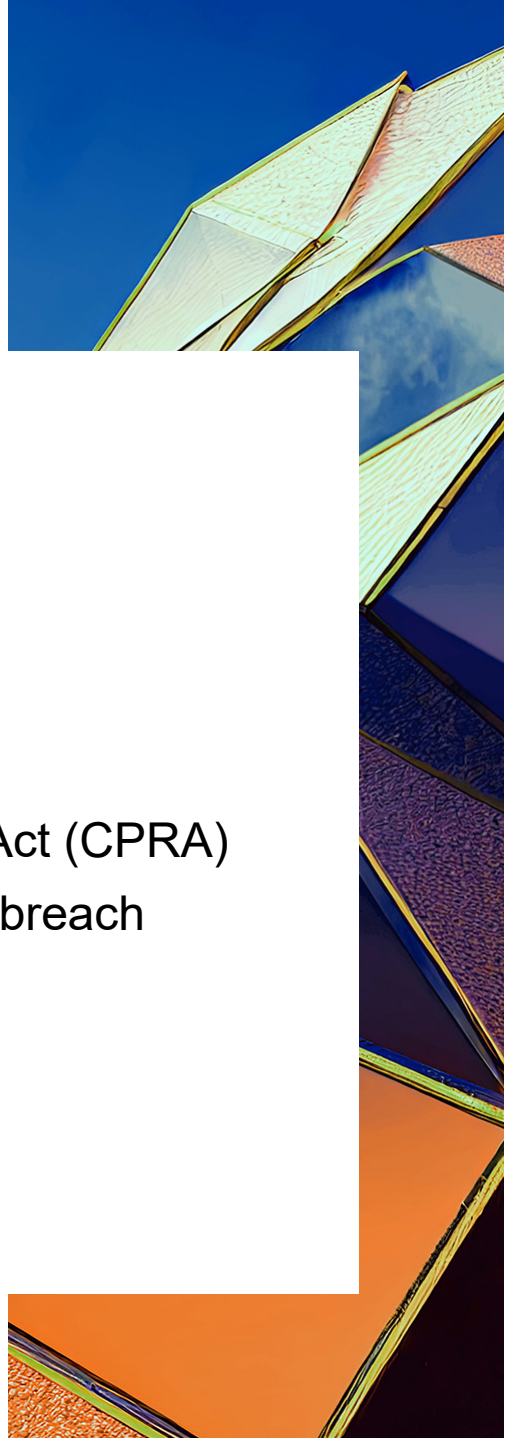
FOLEY.COM

Comprehensive US Privacy Laws



Additional Legislation

- Federal Trade Commission (FTC) under § 5(a) of the FTC Act
- Securities and Exchange Commission (SEC)
- Gramm-Leach-Bliley Act (GLBA) and its implementing regulations
- Health Insurance Portability and Accountability Act (HIPAA)
- New York's SHIELD Act
- California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA)
- All 50 U.S. states plus Washington, D.C. and three federal territories have in place data breach notification laws
- Cybersecurity Information Sharing Act (CISA)
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)



FOLEY

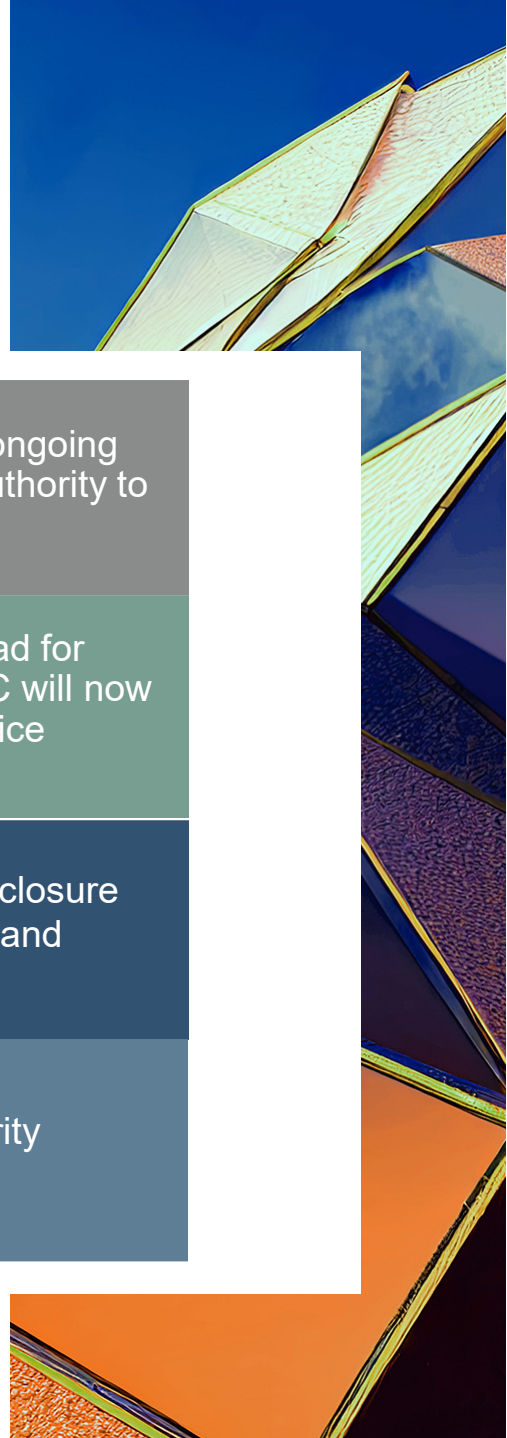
FOLEY & LARDNER LLP

Potential Legal Liabilities

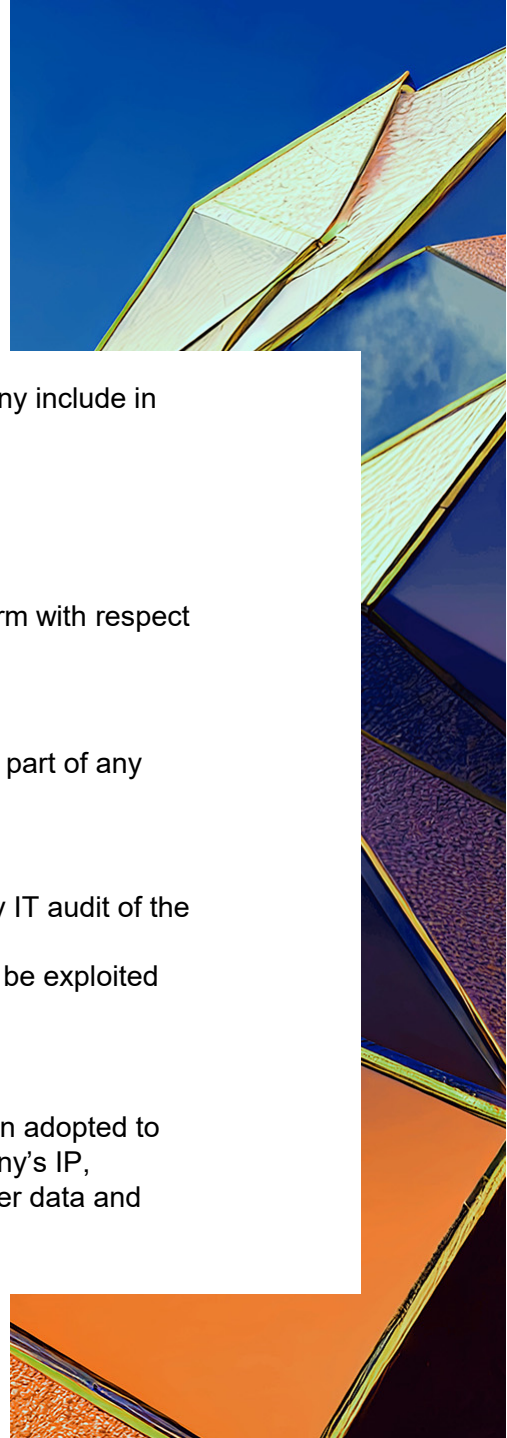
FOLEY.COM

Sources of Corporate Liability After a Security or Privacy Incident

FTC ENFORCEMENT ACTIONS	These actions often lead to settlement or a consent decree, including fines and ongoing monitoring. Wyndham has challenged the Federal Trade Commission's (FTC) authority to enforce a company's cybersecurity practices
FCC ENFORCEMENT ACTIONS	The Federal Communications Commission (FCC) generally follows the FTC's lead for telecommunication companies and other companies within its authority. The FCC will now regulate broadband providers under the new FCC ruling that brings internet service providers under Title II of the Communications Act
SEC ENFORCEMENT ACTIONS	There have been no enforcement actions yet, but the SEC has indicated that disclosure requirements for public companies also include disclosure of cybersecurity risks and cybersecurity incidents
STATE ATTORNEYS GENERAL	State attorneys general enforce state privacy, breach notification, and data security laws (when applicable)

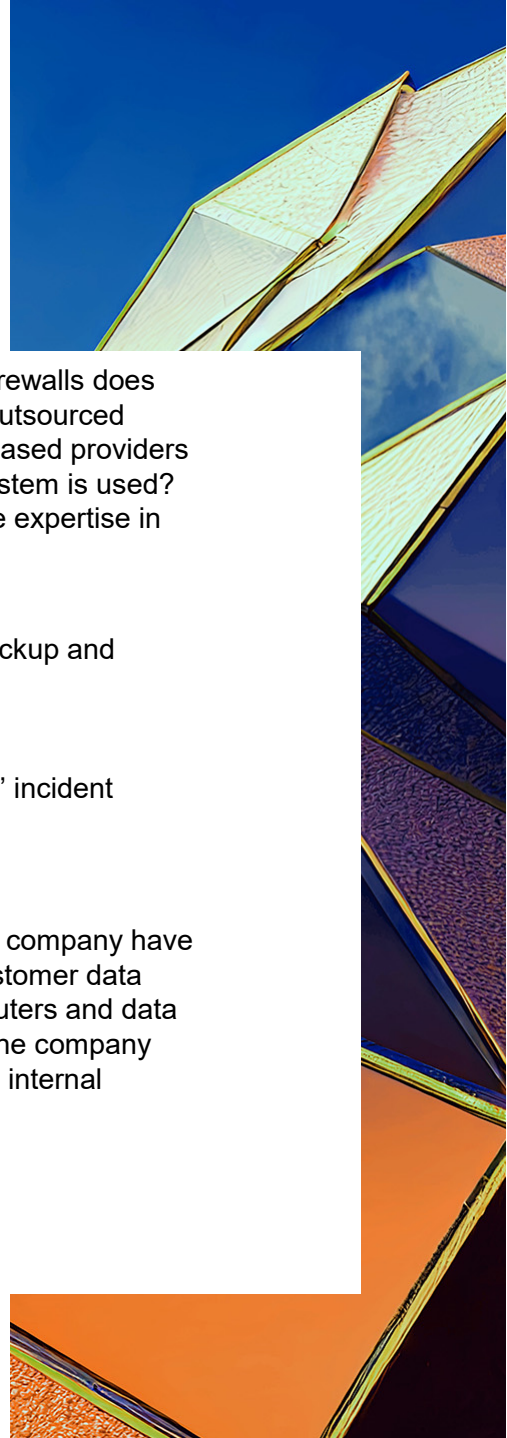


Cybersecurity Due Diligence for Directors and Officers



1. What are the greatest cyber security threats and risks to the company's highest-value intangible assets, and the most sensitive company and customer information? Does the company's risk management and assessment deal with protecting those assets and that information?
2. What is the company's volume of cyber security incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? How much time and cost is incurred to respond to those incidents?
3. What would the worst-case cyber incident cost the company in terms of lost business, system downtime, and reputational damage?
4. What is the company's specific cyber security breach response and crisis management plan, and how will it respond to customers, clients, vendors, the media, regulators, law enforcement, and shareholders, traditional and social media, NGOs, bloggers? Have the plans been practiced in mock situations?
5. What cyber security training does the company include in its compliance program?
6. What due diligence does the company perform with respect to its third-party service providers?
7. What cyber security due diligence is done as part of any acquisition?
8. Has the company performed a cyber security IT audit of the company's systems, services and products to analyze potential vulnerabilities that could be exploited by hackers?
9. What infrastructure enhancements have been adopted to show affirmative action to protect the company's IP, intangible assets, sensitive data and customer data and personal information?

Board of Directors Risks Assessment Questions



1. Where is the company's data stored geographically, and in what data centers? Has the General Counsel examined the legal issues in each jurisdiction?

2. What is the computer architecture structure of the company's computer centers and data centers, are they accessible to company employees, customers and vendors and suppliers, and how? Are they accessible to mobile users and how? What computer and data centers are outsourced, and how? How much data has been placed into a cloud computing environment, in what architecture, and are the clouds being used private, public, or a hybrid? Given all the retail data breaches, does the company utilize point of sale terminals and are they being updated? Does the company use mobile payment hardware and software?

3. Are company and customer and competitor data being commingled in databases or on servers or in the same cloud environment or kept separate and is either customer or company data exposed to competitors, vendors, suppliers or other parties? If so, what types of security measures or confidentiality agreements been implemented?

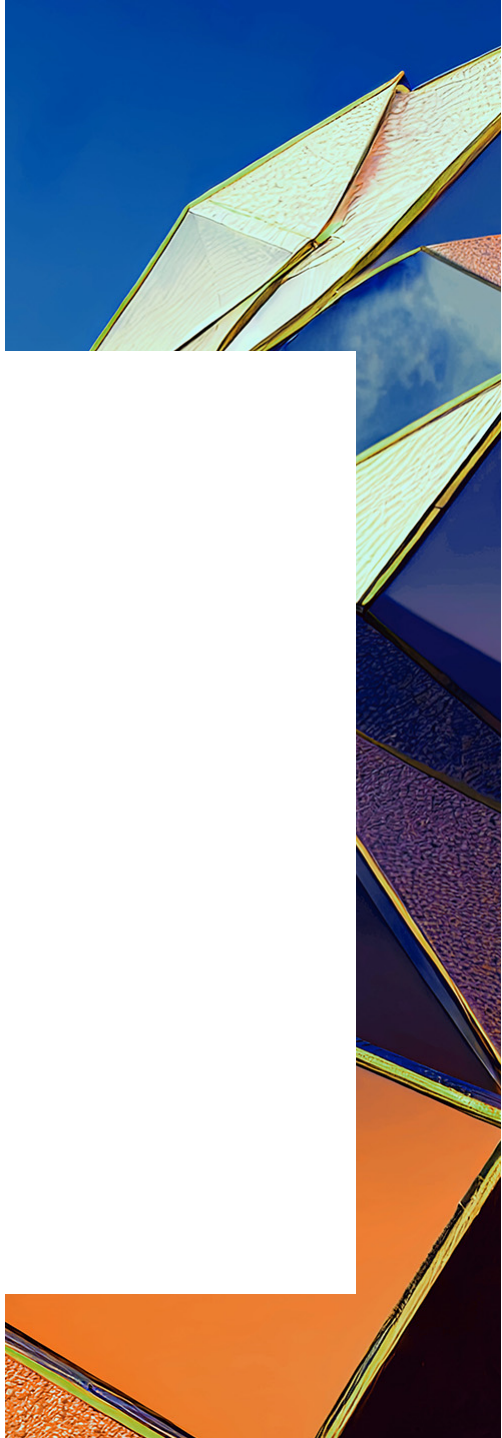
4. What level and type of encryption and firewalls does the computer and data onsite centers, outsourced computer and data vendors and cloud-based providers use? What type of perimeter security system is used? Does the IT team or its consultants have expertise in these systems?

5. What are the company's and vendors' backup and disaster recovery plans?

6. What are the company's and the vendors' incident response and notification plans?

7. What speed and level of access does the company have to security information on its data and customer data stored in company and outsourced computers and data centers and cloud locations in the event the company needs to respond to a regulatory request, internal investigation or litigation?

Board of Directors Risks Assessment Questions



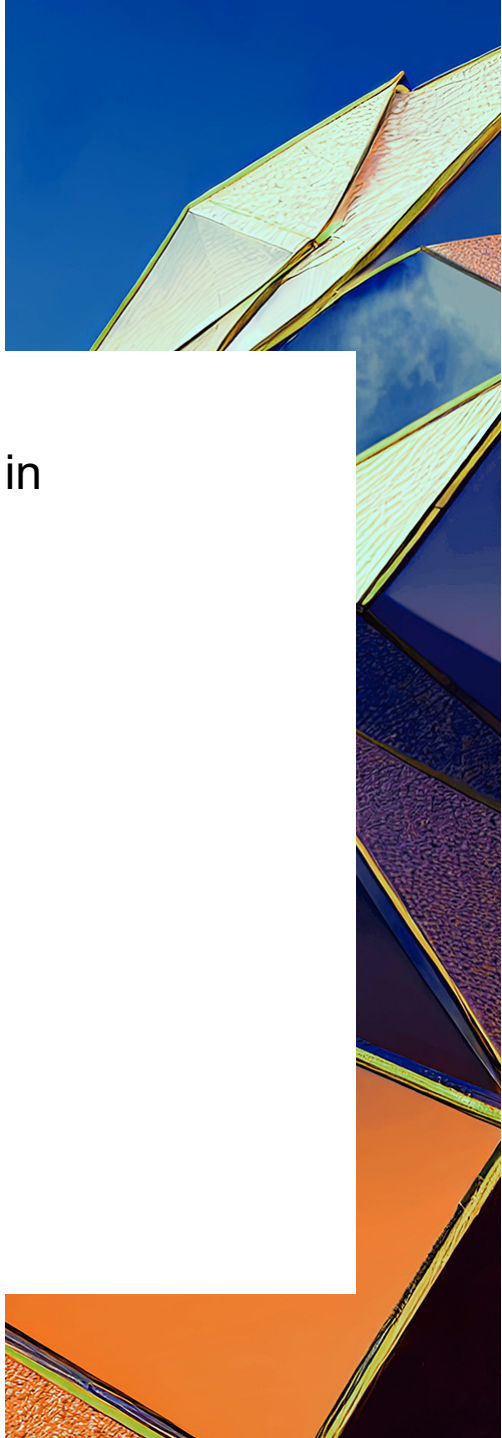
8 How transparent are the vendor and cloud providers' own security systems? What access can the company get to the cloud provider's data center and personnel to ensure the security system is in place and functioning, while also making sure it can make a risk assessment and design a response plan?

9 What are the vendor and cloud servicers' responsibilities to update their security systems as technology and sophistication evolves?

10 What are the company, computer and data vendors, and cloud providers' ability to continuously monitor, detect, and respond to security incidents, and what logging information is kept in order to potentially detect suspicious activity?

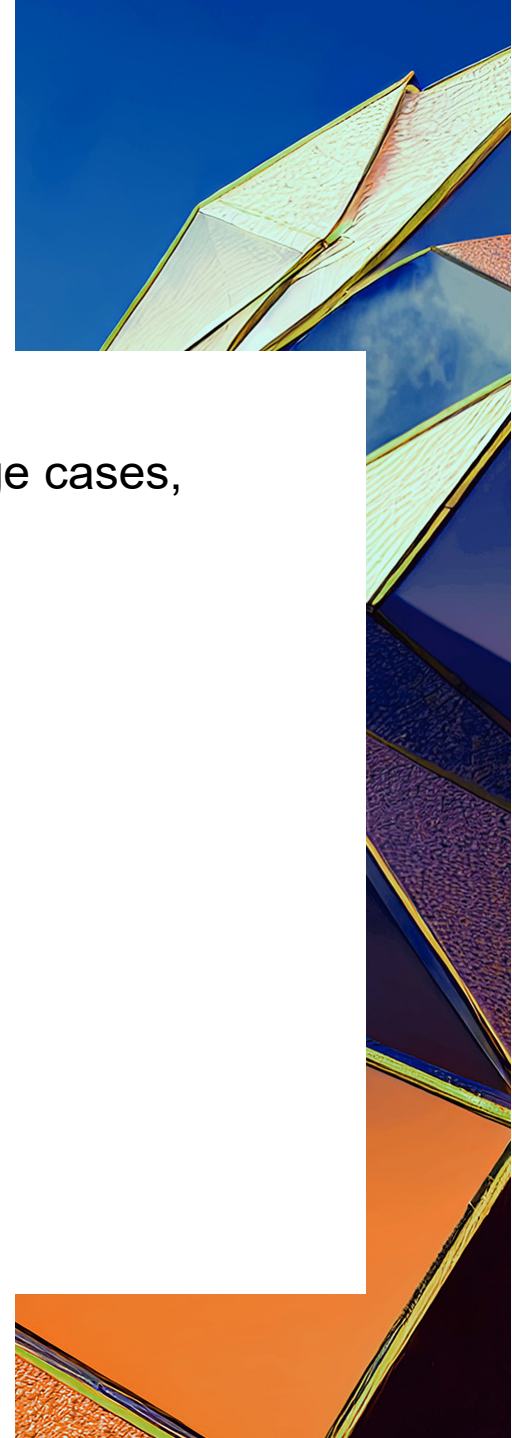
Director and Officer Liability

- Shareholders also may file lawsuits alleging that negligence of the directors and officers in addressing cybersecurity risks resulted in financial loss



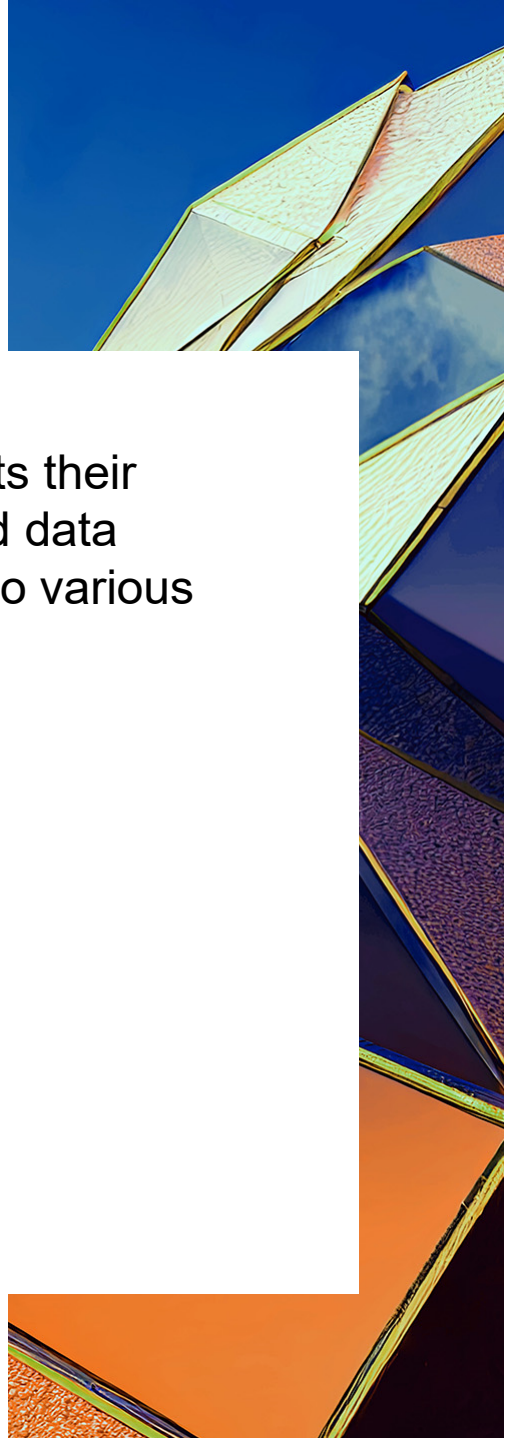
Intellectual Property (IP) Implications

- Cybersecurity incidents involving IP loss or disclosure, particularly in industrial espionage cases, can lead to costly legal liabilities.

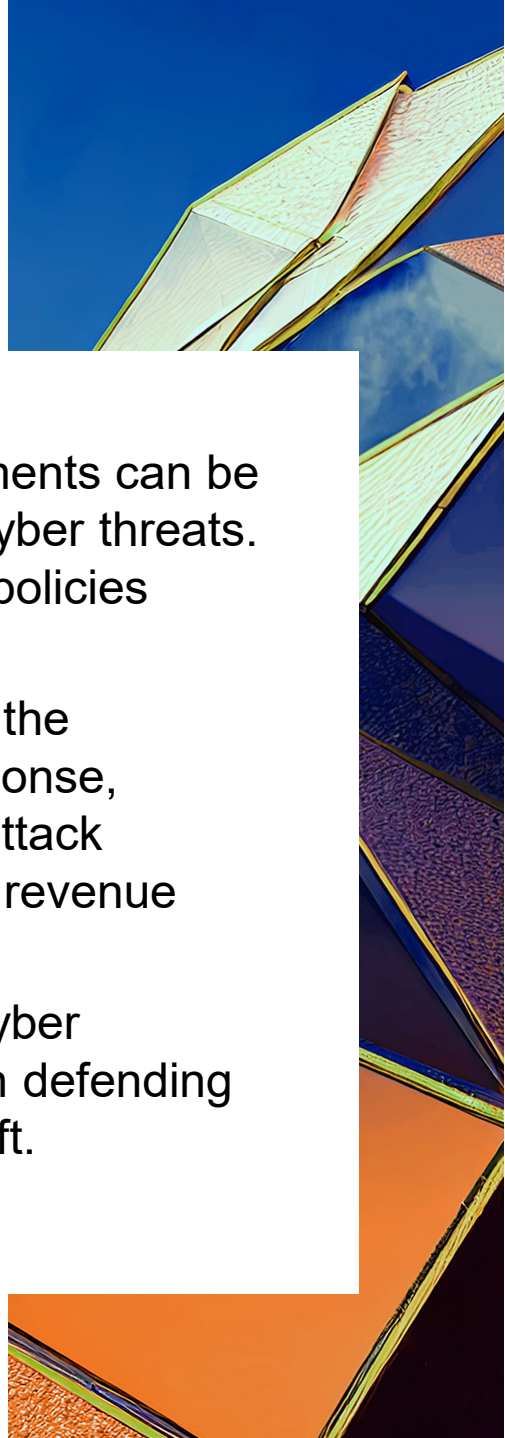


Contractual Obligations

- Manufacturers could be held liable for breach of contract if a cybersecurity attack disrupts their ability to fulfill contractual obligations. Contracts often contain clauses related to required data protection and cybersecurity, and failure to meet these contractual obligations can lead to various legal consequences.



Cyber Insurance Considerations



- Combating the increase in cyber threats and compliance with the growing legal requirements can be costly. Cyber insurance plays a crucial role in mitigating financial risks associated with cyber threats. Manufacturers should carefully consider the various aspects of cyber insurance. These policies typically consist of two main components:
  - First-Party Coverage: This aspect of the policy addresses the direct costs incurred by the manufacturer as a result of a cyber incident. It includes coverage for data breach response, business interruption, and data restoration expenses. For example, if a ransomware attack disrupts operations, the business interruption coverage may help compensate for lost revenue during the downtime.
  - Third-Party Coverage: Third-party coverage deals with liability issues arising from a cyber incident. It encompasses protection against legal costs, such as those associated with defending against lawsuits due to data breaches, privacy violations, and intellectual property theft. Manufacturers may also be covered for regulatory fines and penalties.

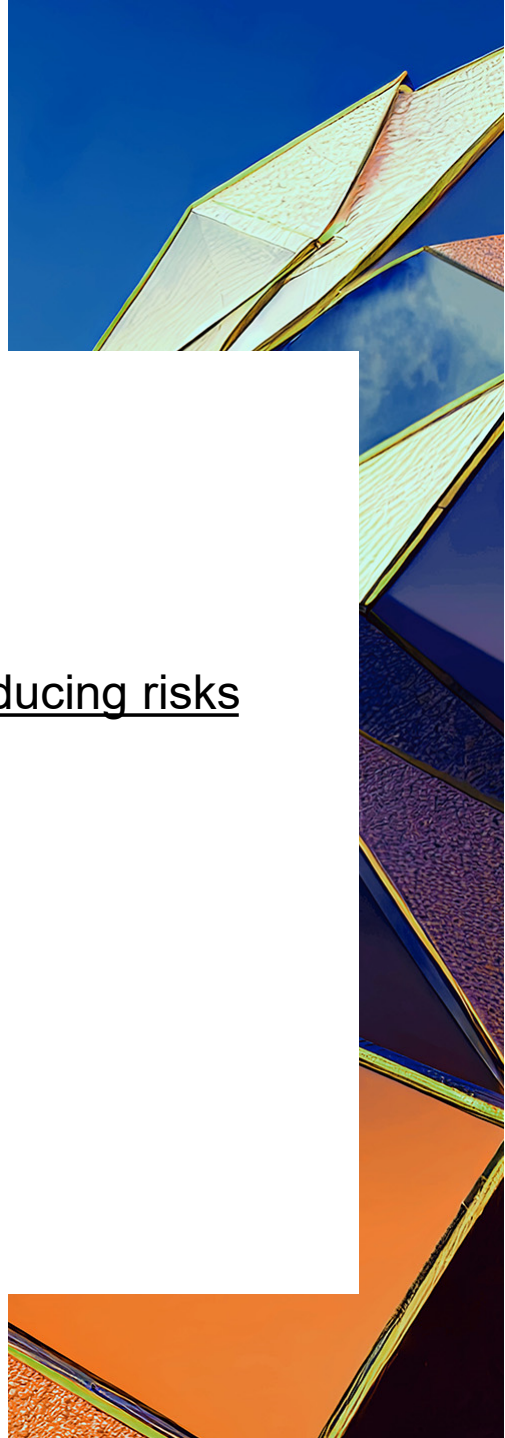
FOLEY

FOLEY & LARDNER LLP

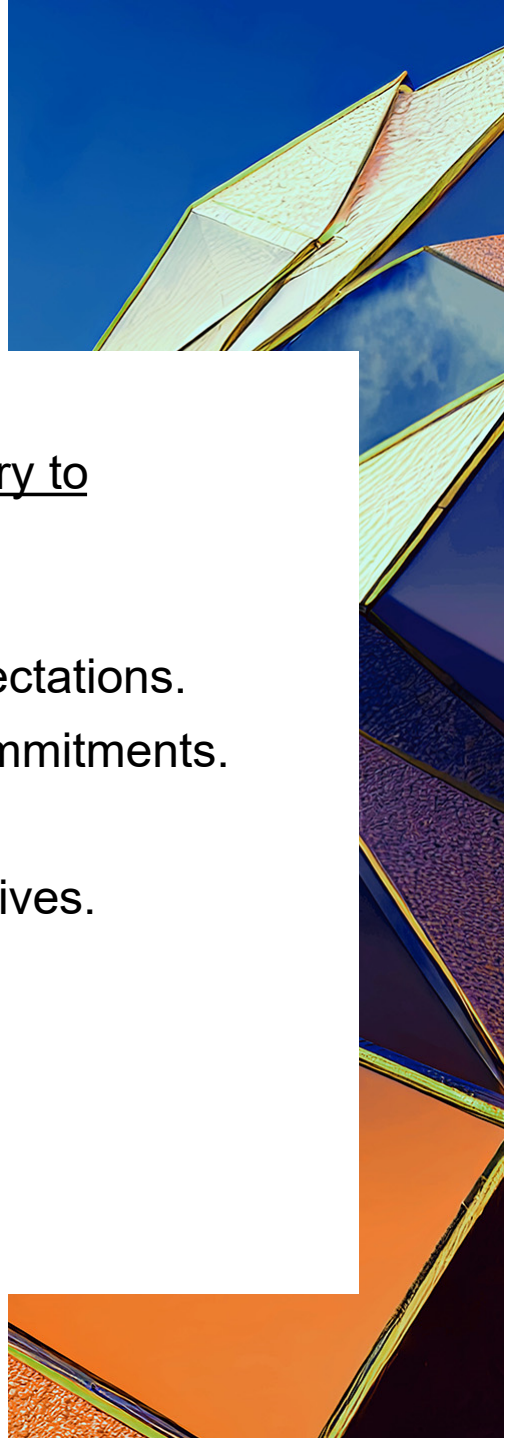
Managing Cyber Risks Today

What is Cybersecurity Strategy?

- How your organization reduces your risks
- Use a standard of practice *to measure risk*, addressing risks to others and yourself
  - Duty of Care Risk Analysis (DoCRA), CIS RAM, ISO 27005, NIST 800-30
- Use a standard of practice to determine roles, responsibilities, processes, metrics for reducing risks
  - ISO 27001, NIST Risk Management Framework
- Ensure that risk measurement, reduction, and reporting are integrated into the business



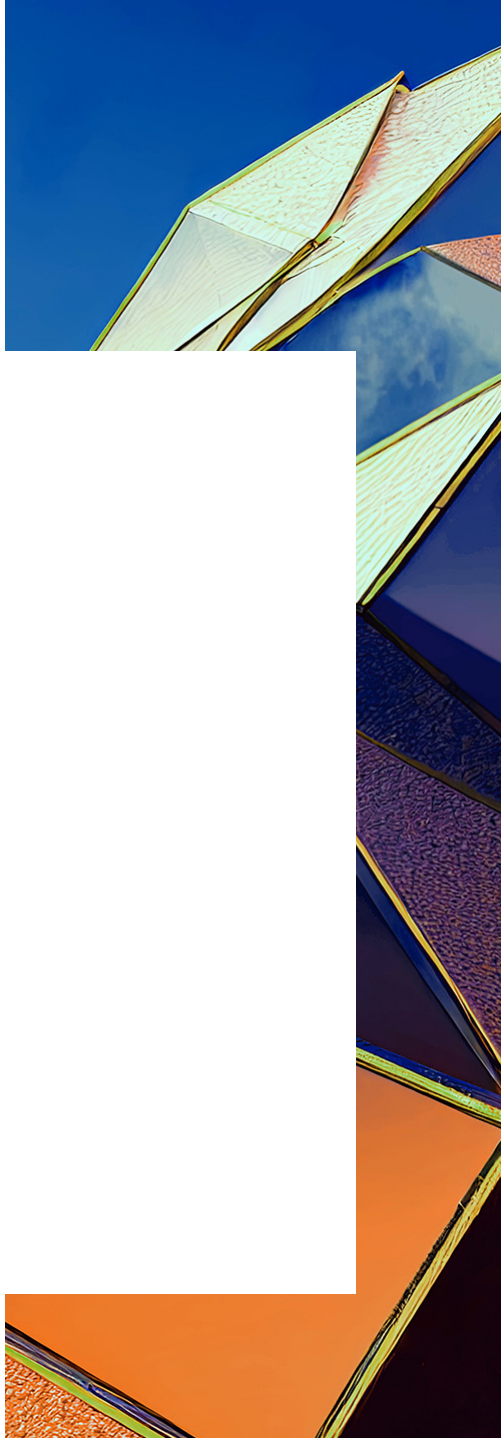
What is Governance?



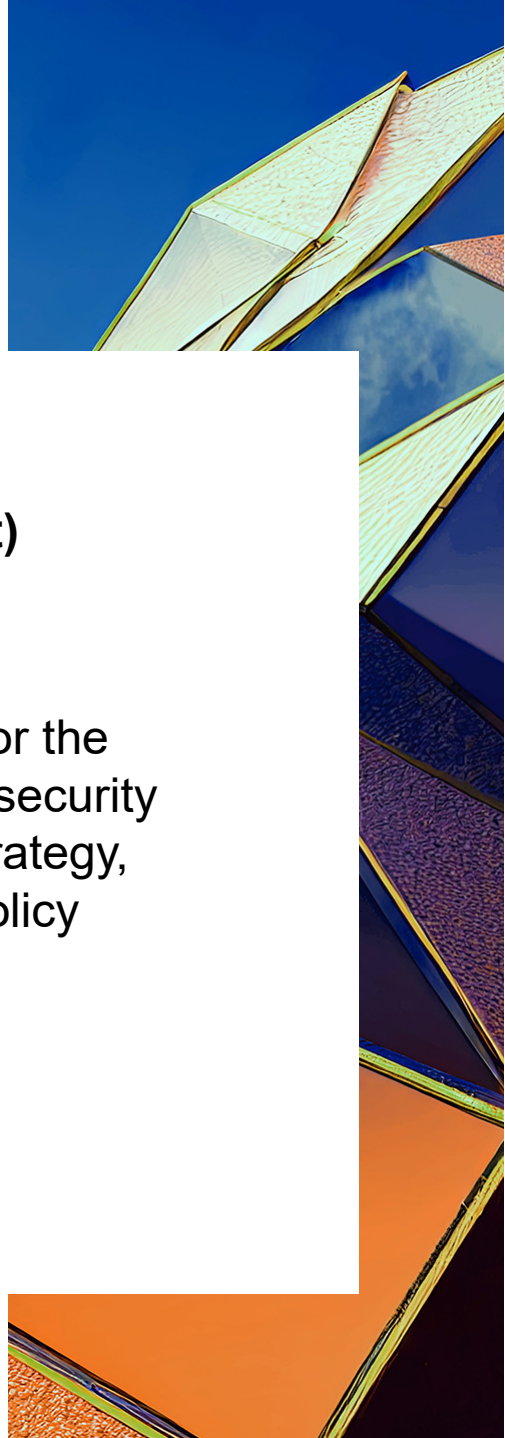
- Responsibilities for cybersecurity are at the level of management whose role is necessary to effectively manage the risk.
  - Executives:
    - Gather and communicate responsibilities; contracts, regulations, and business expectations.
    - Ensure that resources, prioritization, and collaboration are sufficient for meeting commitments.
  - Management:
    - Communicate expectations to personnel. Communicate status and needs to executives.
    - Ensure that teams, projects, and systems meet commitments.
  - Personnel:
    - Implement and manage controls according to commitments.
    - Report status and security concerns.

Why is Governance Rising as a Cybersecurity Issue?

- In breach case after breach case, we see cybersecurity teams unable to communicate with executives
- Executives don’t know what they should know
- Executives do not understand cybersecurity personnel
- Management does not feel comfortable being honest about risks
- Management does not know how to conduct risk analysis in business and legal terms
- Good governance would fix this
- Good governance is good for cybersecurity



The Rise of Governance



SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule

- Disclose what your risk management, strategy, and governance methods are

23 NYCRR Part 500

- Operate a data governance program

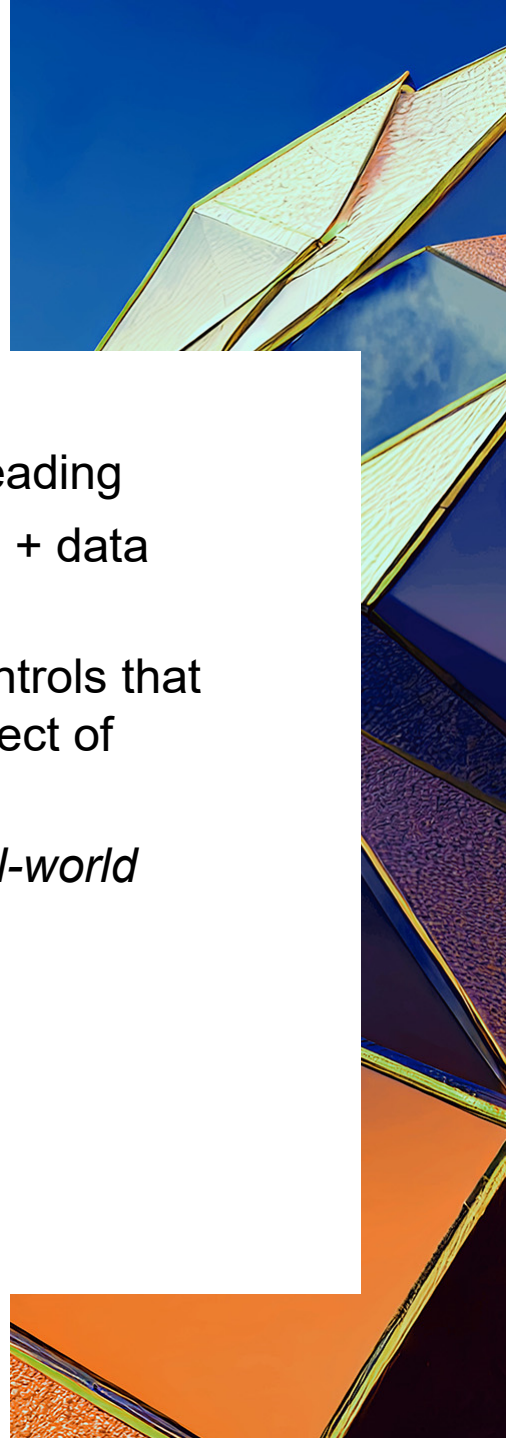
NIST Cybersecurity Framework 2.0 (Draft)

- Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

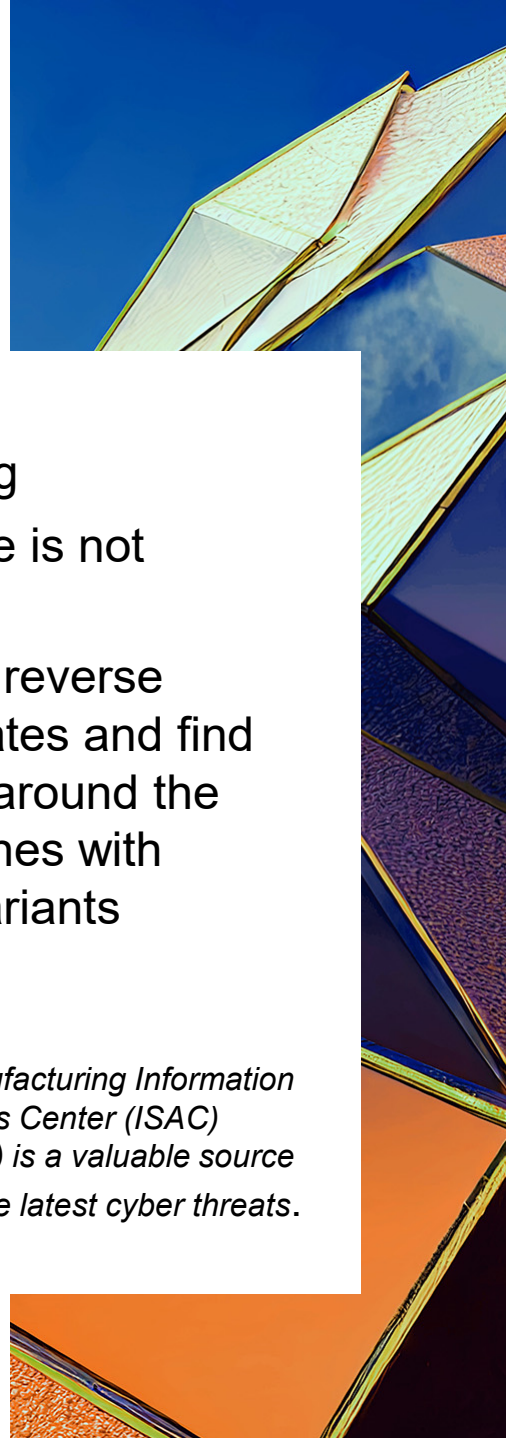
“Secure" Architecture

- Somewhat effective tools exist.
- However:
  - These primarily focus on preventing intruders from accessing the network (“keep the bad actors out” or “perimeter defense”)
    - Include firewalls, intrusion detection and prevention systems, secure access control, and air gapping
  - Controlling access to the network, manufacturers can reduce the likelihood of a breach.

- “Secure Architecture” can be misleading
  - Conjoining of perimeter defense + data security;
  - Involves inadequate security controls that are applied only to a limited aspect of operations or a supply chain;
  - *Little or no consideration for real-world physical consequences*;
  - Aligned solely with compliance requirements.



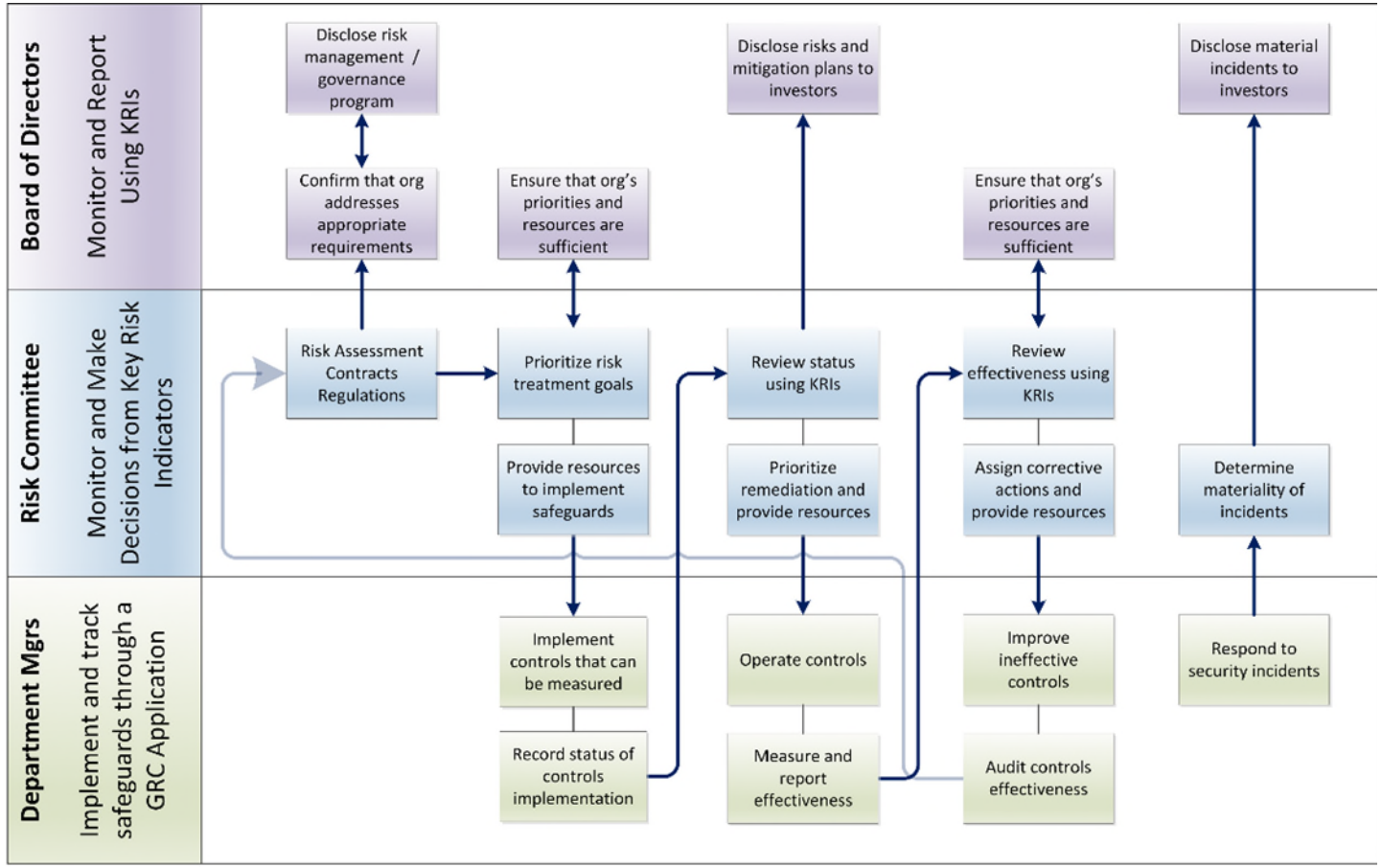
Multi-Faceted Approach to Cybersecurity

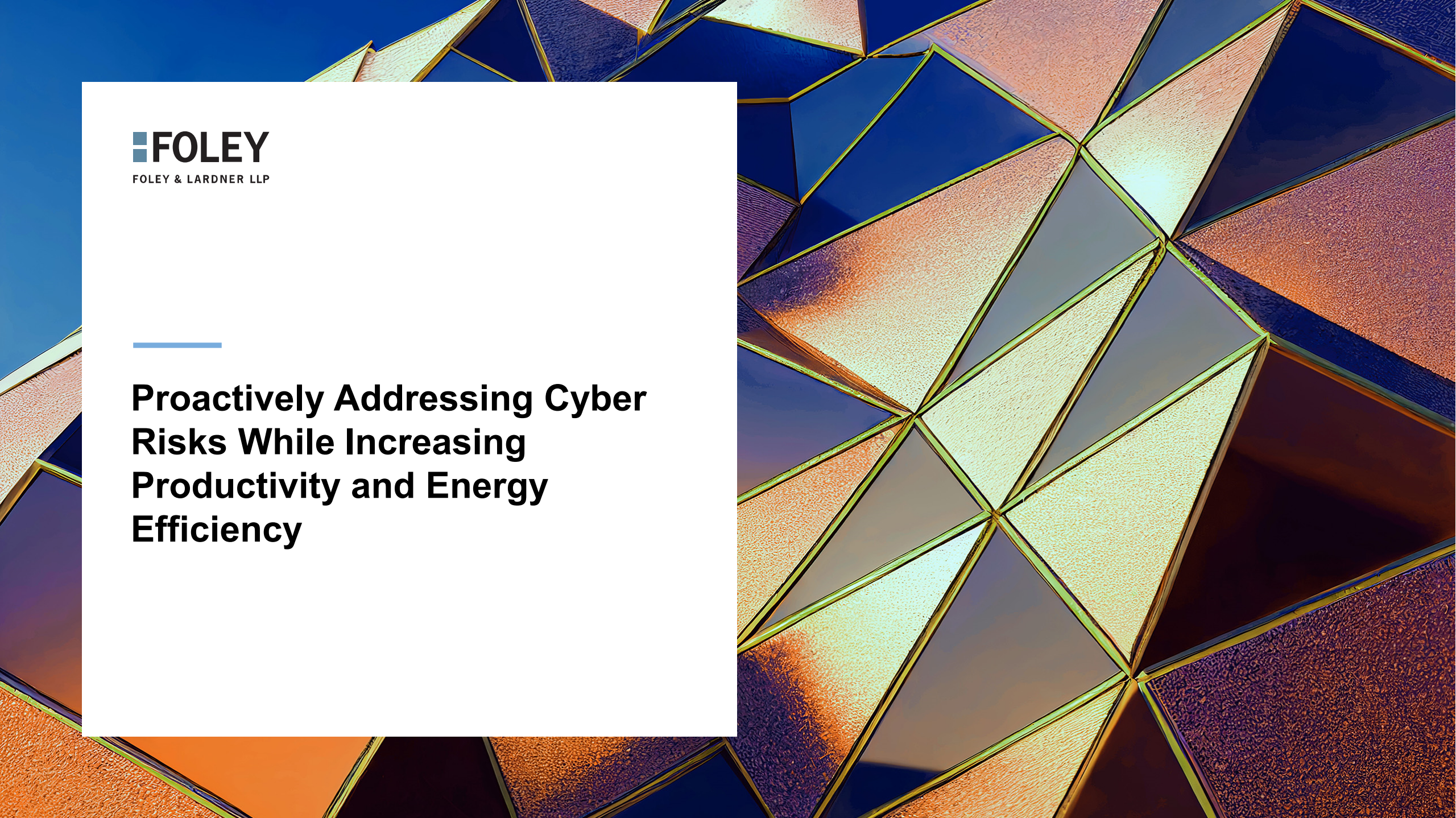


- Investing in employee cybersecurity training and awareness
  - Human element represents the single biggest cybersecurity risk
  - First line of defense against cyber threats
- Regular software updates
  - Updates often secure against known vulnerabilities
  - Threat actors target older software vulnerabilities - low-cost compromise
  - Vulnerabilities are old, patches available for years
  - Outdated software harbors thousands of vulnerabilities that cybercriminals exploit
- Active monitoring
  - Patching alone is not enough
  - Attackers can reverse engineer updates and find ways to work around the released patches with new exploit variants

A recently launched Manufacturing Information Sharing and Analysis Center (ISAC) (https://www.mfgisac.org/) is a valuable source of public information on the latest cyber threats.

Information Flow for Good Governance





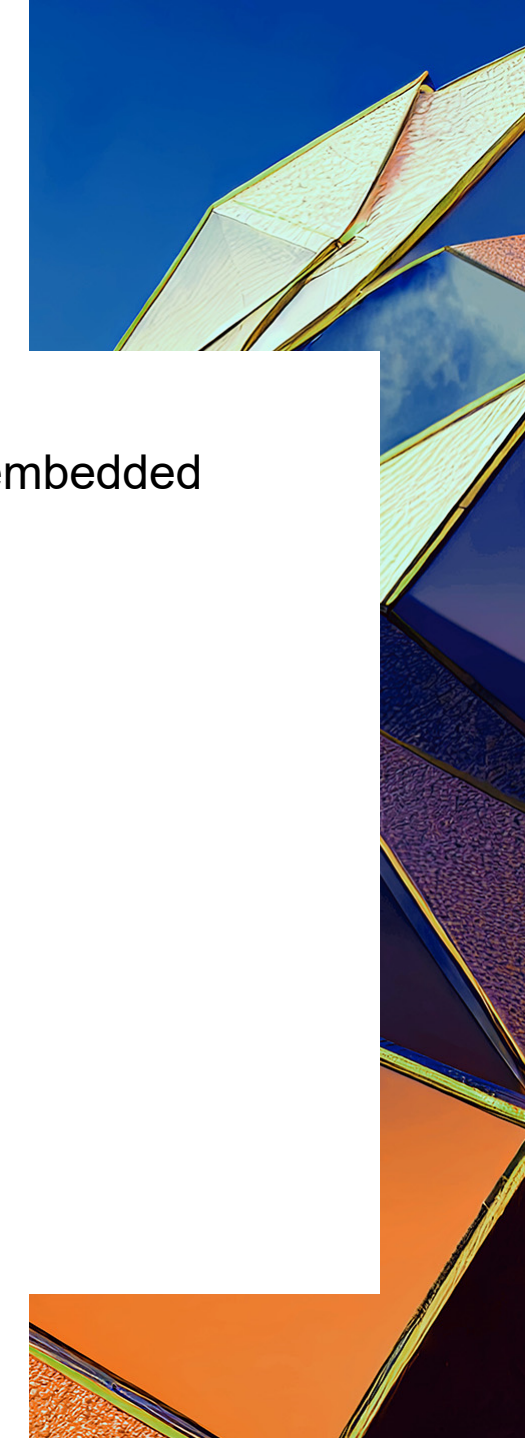
FOLEY

FOLEY & LARDNER LLP

Proactively Addressing Cyber Risks While Increasing Productivity and Energy Efficiency

CyManII's Vision

- To secure U.S. manufacturers as they digitize by fortifying their physical systems with embedded cybersecurity and energy-efficient solutions.



Core Pillars

Inspire

Innovate

Inform

Secure the digital thread

- Build defensible architectures
- Create identify-centric cyber-physical passports
- Secure a decarbonized ecosystem

Secure.*TOGETHER*

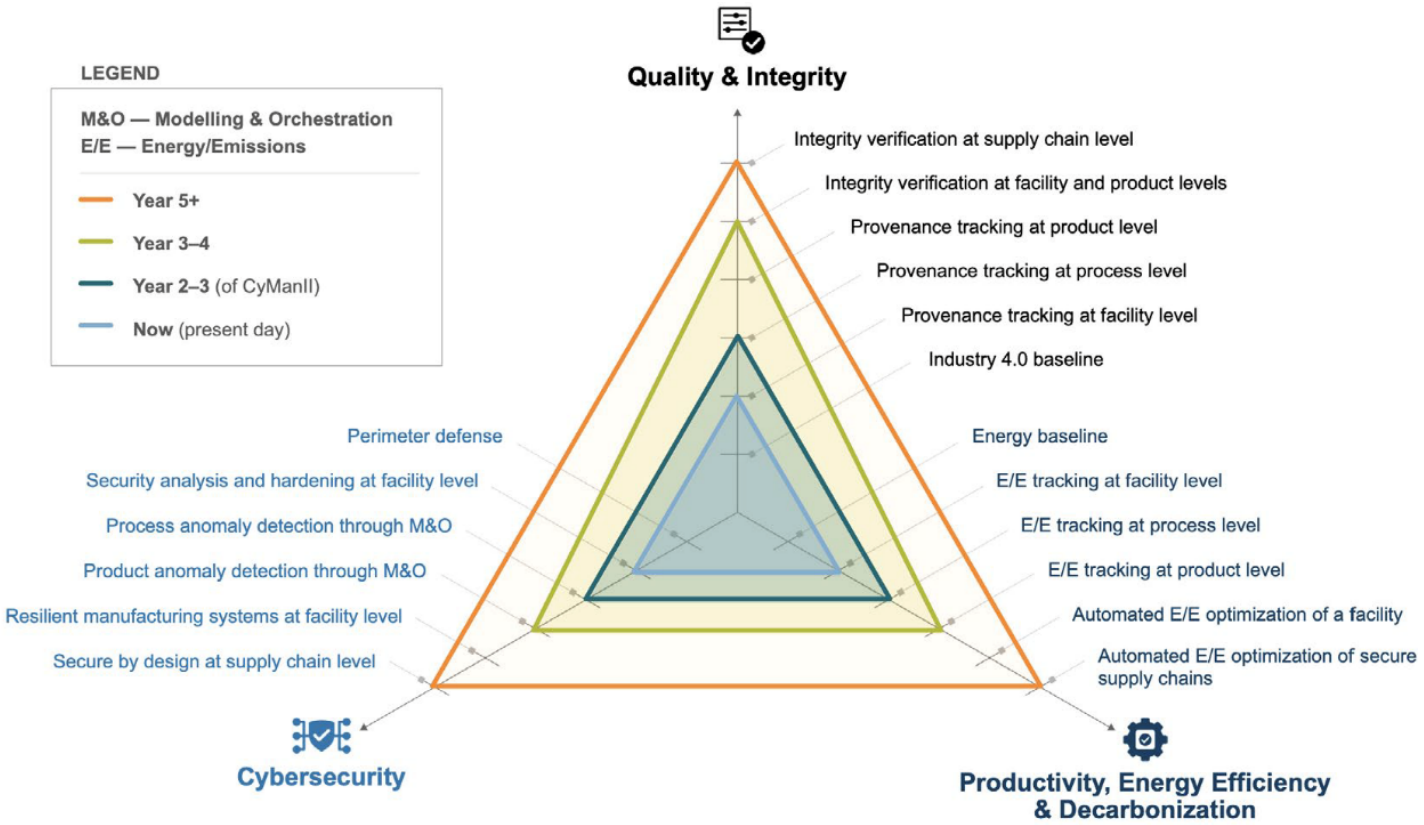
- Partner across industry's supply chain
- Cooperate across Govt stakeholders
- Focus on:
  - Manufacturing Sectors
  - Critical Energy Infrastructure
  - Data and beyond…

Create a cyber-informed workforce

- Focus on OT / ICS security
- Leadership on CIE
- Empower current workers
- Expand emerging workforce (students)

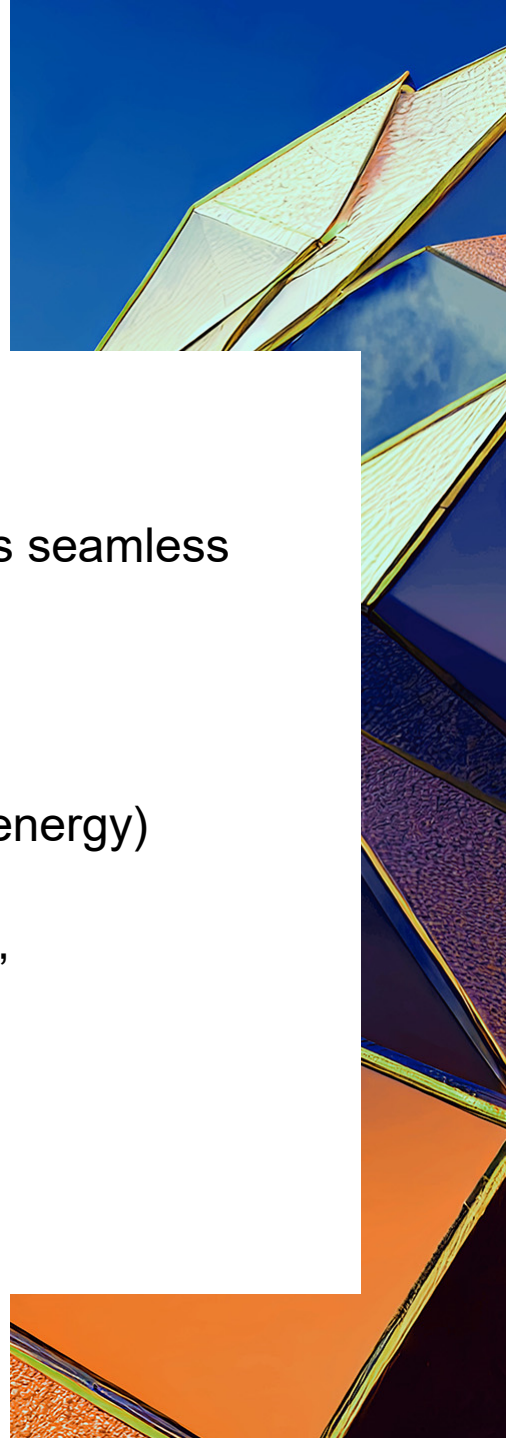
CYMANII the cybersecurity manufacturing innovation institute

Innovations Needed to Fundamentally Cyber Secure IT/OT/ICS and Physical Systems While Moving from Cyber Investments as a Cost Center to a Profit Center

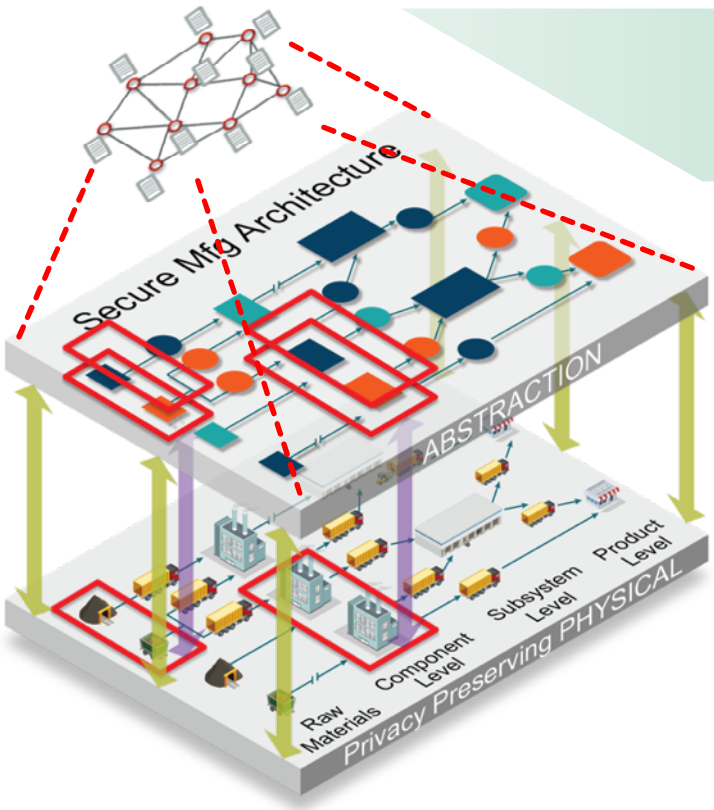


CyManII's Secure Defensible Architectures

- The Digital Engineering Lifecycle must be addressed across the entire supply chain
  - Every operation, machine, and person is a "node" in this digital design (supply chain is seamless with operations)
  - Every node is captured in a cyber-physical identity (passport) that is used for:
    - Guarantees of physical functions
    - Linkage of security to product quality and energy / emissions efficiency (embodied energy)
  - Verifiable security properties that are extensible to multiple domains
- Cyber-Physical Passport: makes your supply chains "born qualified" and "rooted in trust"



Secure Defensible Architectures (SDA)



Analysis
Modeling
Optimization

- **Maximize E&E Efficiency**
- **Maximize Production**
- **Minimize Risk**

Integrated Model of Automation & Supply Chain

- Perimeter defenses insufficient in modern **digital design lifecycle**
- We treat **Automation as nodes in Supply Chain** network

Framework for Security & Efficiency Across "Sectors"

- Digital **identity** = physical + cyber + energy (Cyber-Physical Passport)
- Automation **activities** validated across supply chain

Agile, Adequate, & Consequential Formalism to Validation

- **Targeted formal methods** and evidential basis for design & implementation
- Continuous Integration/Deployment (**CI/CD**) in manufacturing context

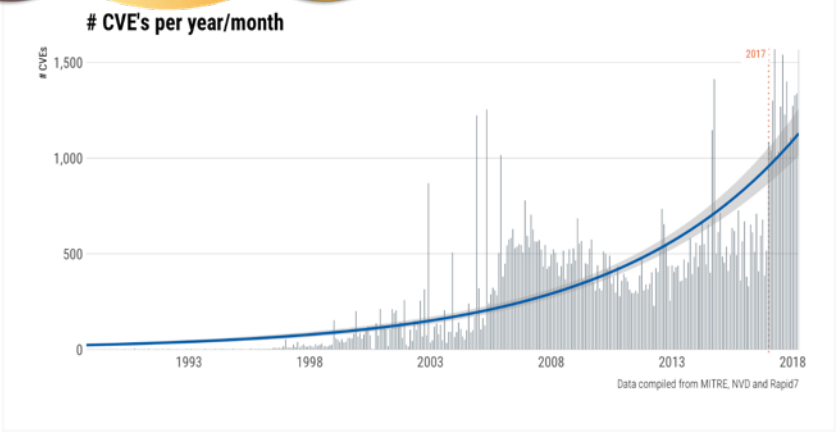
Unify security across the digital thread of design, build, deliver for industries of all sizes

Cyber-Physical Passport

- Enables digital provenance tracking through *verifiable security guarantees*.
- Traceability across supplier boundaries.
  - Using a global ledger as well as physical and virtual watermarks, the CPP follows a product through its value chain, crossing suppliers and staying with the end product.
- Verification of the digital thread.
  - Formal verification methods are used to continually assess the critical code along the product's lifecycle for accuracy and evidence of compromise.
- Tamper-proof ledger.
  - The data captured in the CPP is protected and anonymized with use of a unique hash and permissioned blockchain where entities logging transactions are first authenticated.
- Improved protection & system hardening.
  - A secure manufacturing architecture along with a multi-physics digital twin provide enhanced cyber protection and high-fidelity monitoring.

How to Address Cyber Vulnerabilities "At Scale"

- Challenge:
  - Vulnerability trends significantly favor the attackers, present systems are not "defensible".
  - If we continue to reactively chase and patch vulnerabilities, we will "lose the war" for national & economic security.
- New Approach:
  - Identify Cyber Weakness Enumerations that capture thousands of vulnerabilities at a time (1:10,000+)
  - Create methods and tools that can systematically identify and eliminate/mitigate weaknesses
  - Address these CWE's in a priority fashion to cyber secure US Manufacturing
- Current defenses are orders of magnitude behind:
  - 10's days vuln-to-exploit, 100+ days to patch, 200+ days to detect
  - 10's active vulnerability instances / device, 100-1000 latent vulnerabilities
  - 100x the cost to fix in implementation vs design



4/2018 100k CVEs, ~600 CWEs
4/2023 214k CVEs, 933 CWEs

Across 1,063,482 platforms

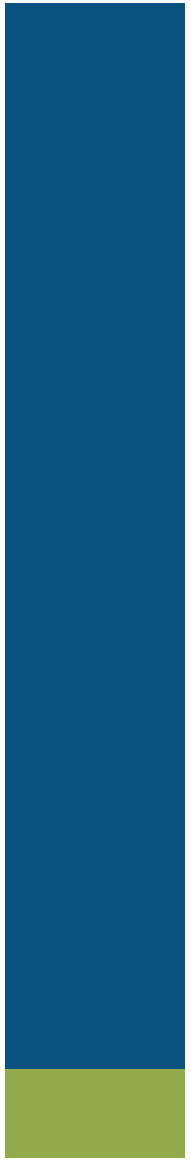
100s to 1000s : 1 of CVEs-to-CWEs

CYMANII the cybersecurity manufacturing innovation institute

U.S. DEPARTMENT OF ENERGY

Workforce Development

- Why 1 million workers?
- We must aggressively reach the growing workforce with training that scales.



13 million

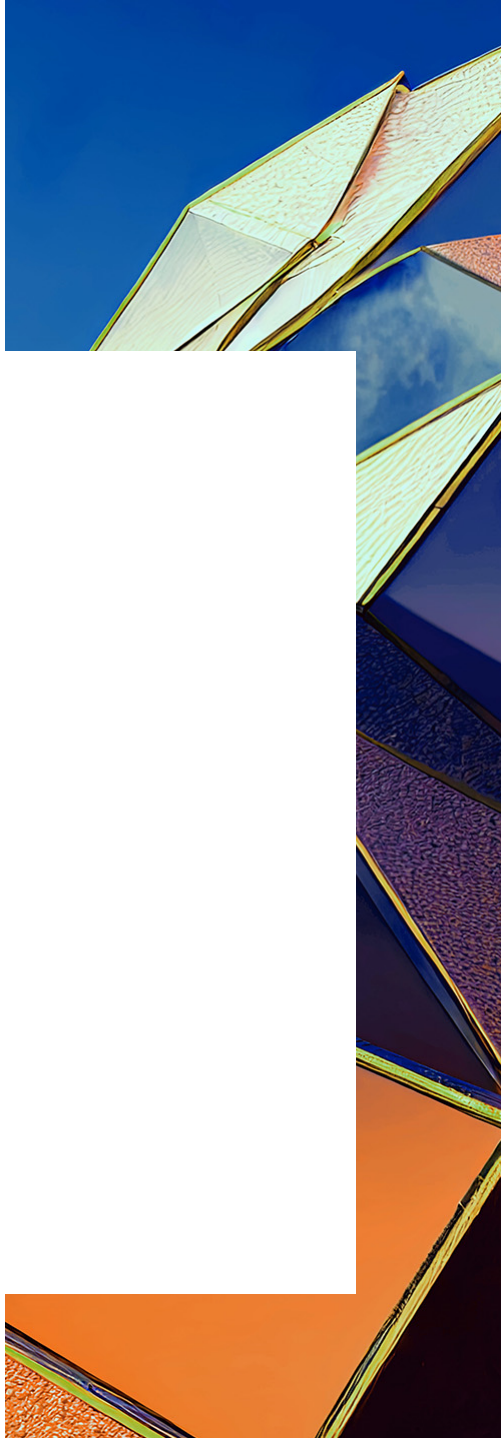
manufacturing workers in March 2023

7.6%

Of the US manufacturing workforce

CYMANII the cybersecurity manufacturing innovation institute

U.S. DEPARTMENT OF ENERGY



Workforce Development

CYBER READINESS INSTITUTE

1

LEADERSHIP & AWARENESS TRAINING

Manufacturing leaders & stakeholders

TOOLINGU | sme

2

CORPORATE ONLINE CYBER TRAINING FOR ALL WORKERS

All manufacturing workers

PORT SAN ANTONIO

3

HANDS-ON COMPLIANCE TRAINING

Information security team & leaders

Networking Academy

4

ONLINE AUTHENICATED TECHNICAL TRAINING

Skilled IT/OT security & maintenance professionals

5

DEGREE AND CERTFCATE SEEKING STUDENTS AND PROFESSIONALS

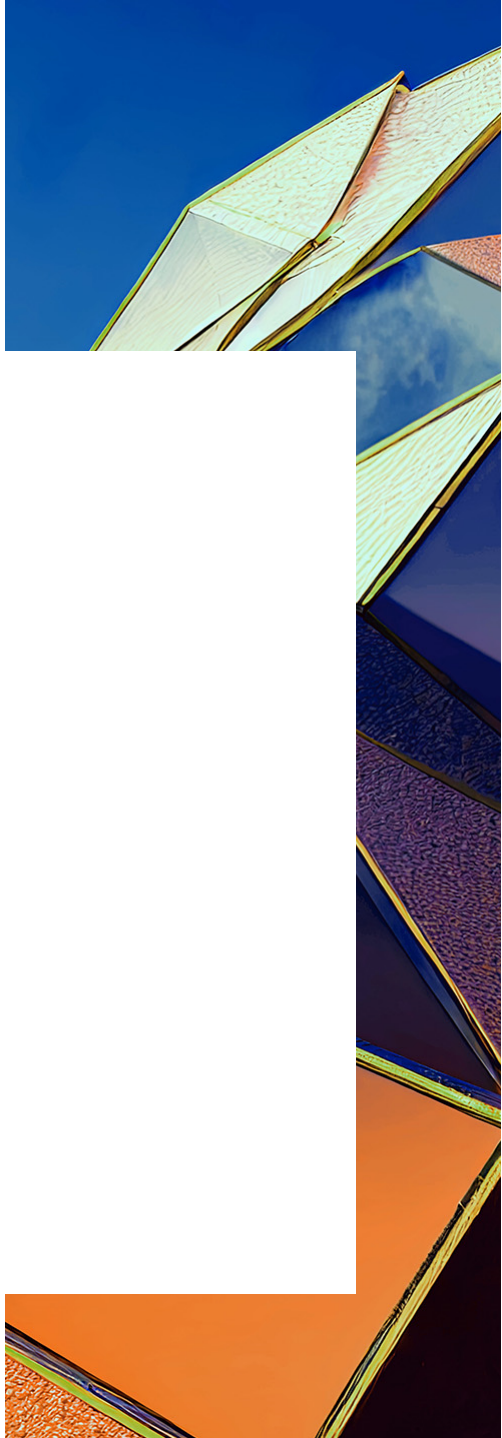
Online degree & certificate seeking students and professionals.

CYMANII the cybersecurity manufacturing innovation institute

U.S. DEPARTMENT OF ENERGY

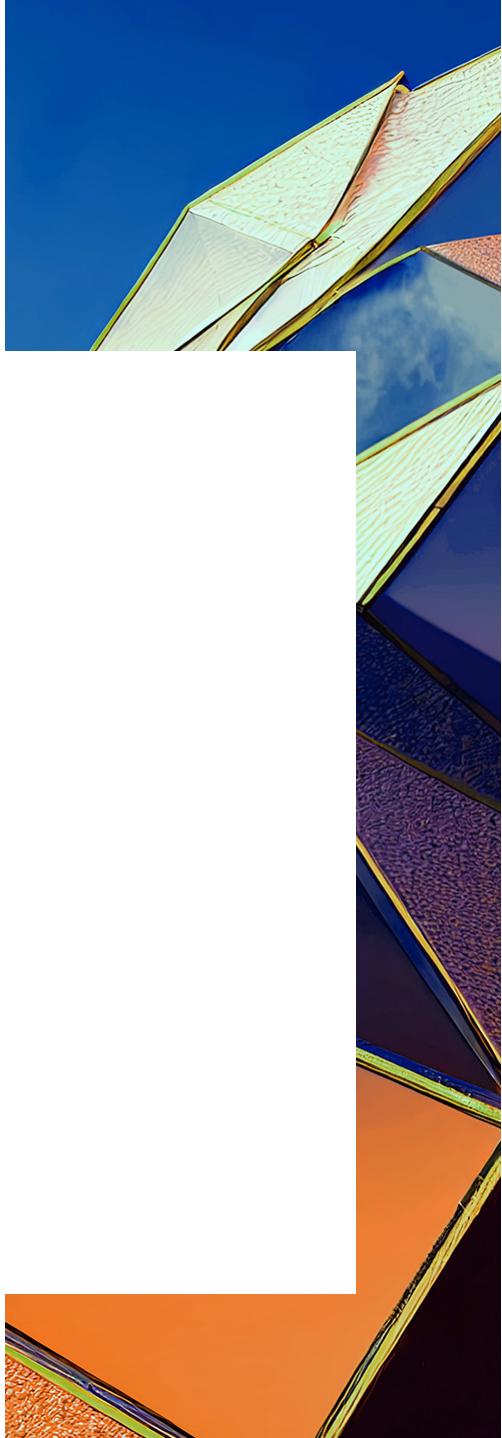
Thank You

- Questions?



About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.



FOLEY

FOLEY & LARDNER LLP

FOLEY.COM

FOLEY

FOLEY & LARDNER LLP

Break

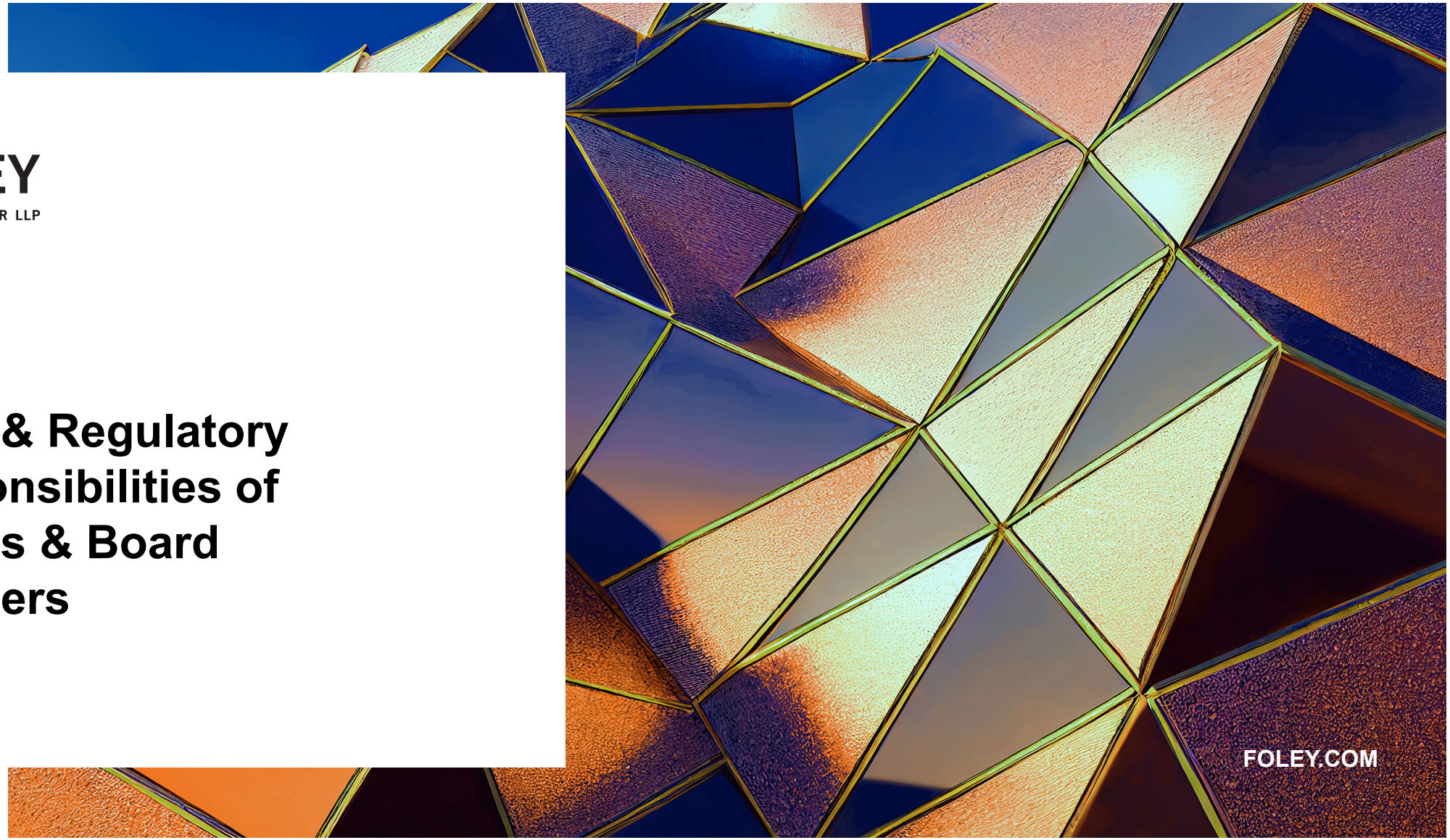
Presentations will resume shortly

FOLEY

FOLEY & LARDNER LLP

Legal & Regulatory Responsibilities of Boards & Board Members

December 7, 2023



Presenters

Beth Boland
Partner | Boston

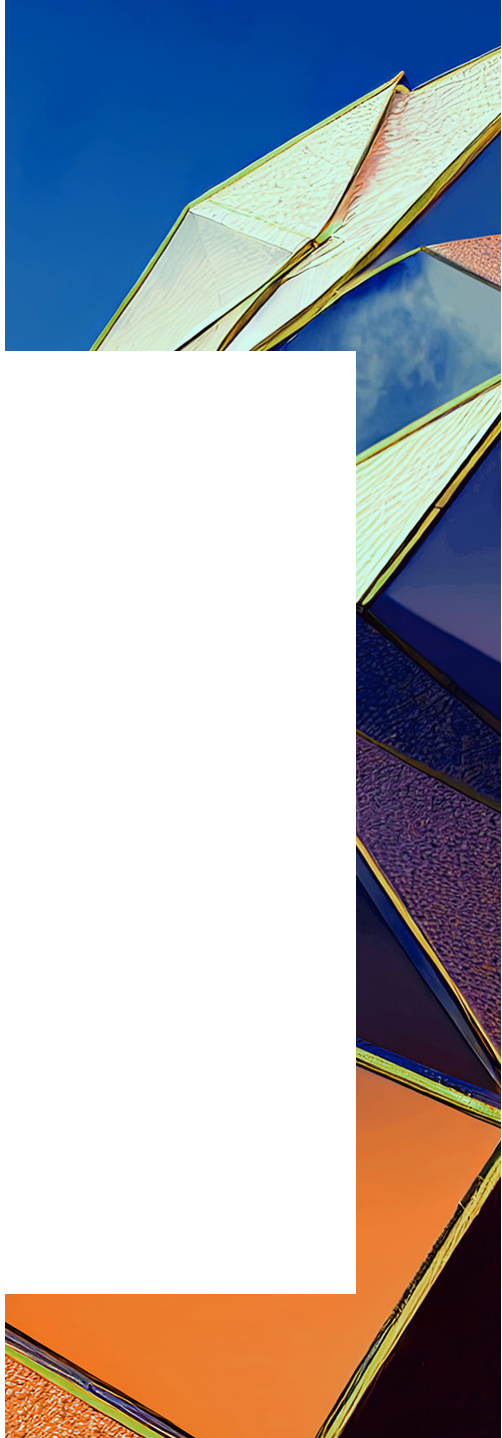
T: 617.226.3179
E: bboland@foley.com

Jessie Lochmann
Partner | Milwaukee

T: 414.297.5817
E: jlochmann@foley.com

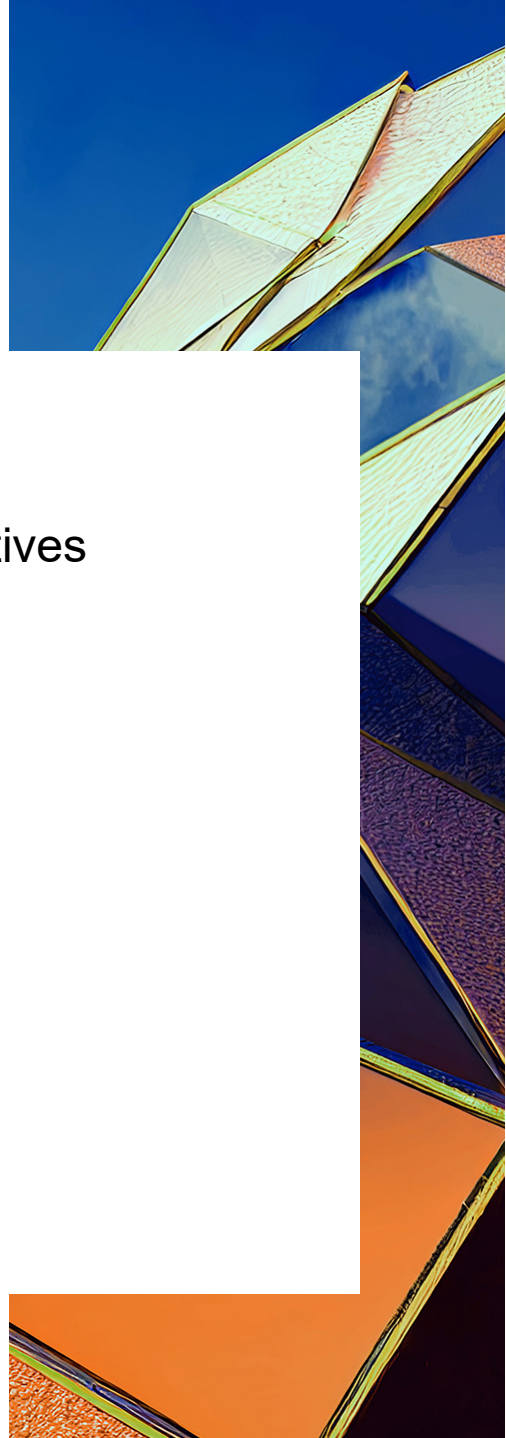
Agenda

- Director’s Legal Duties
- Recent Trends
- Impact of Trends on Board Functions
- Board’s Response to Management in Trouble
- Liability Protections



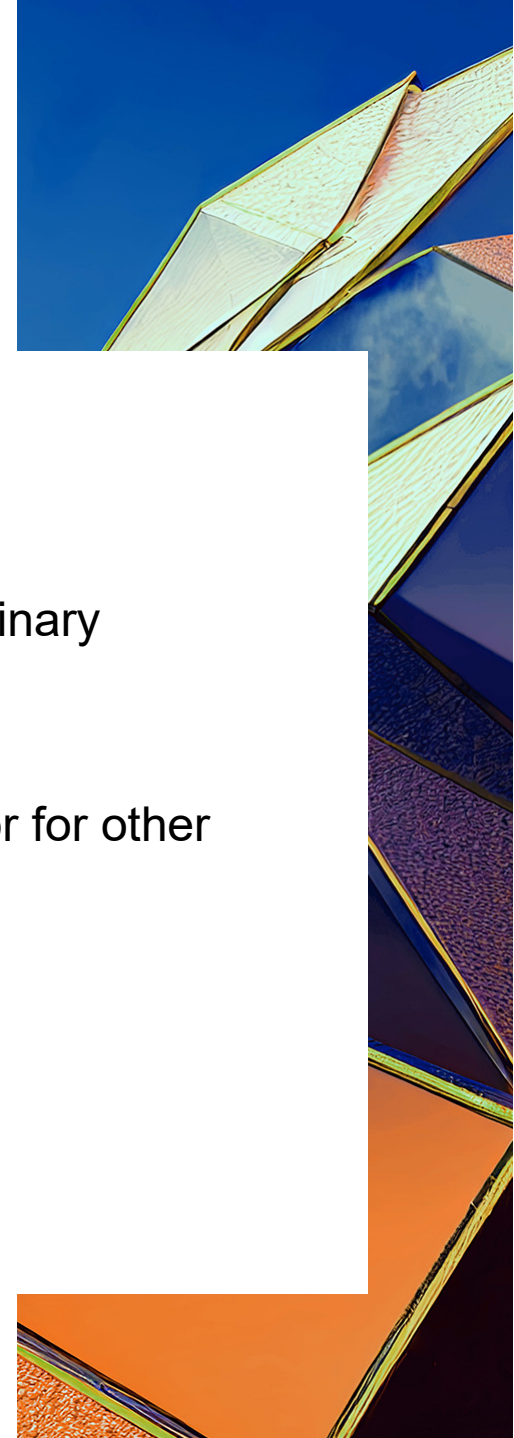
Role of Board - Responsibilities

- Board is responsible for overseeing the business and affairs of its company
  - Approving fundamental operating, financial and corporate plans, strategies and objectives
  - Overseeing risk (*informed* oversight)
  - Evaluating performance of the company and its management
  - Selecting, evaluating, and fixing compensation of corporate officers
  - Preparing for senior management succession
  - Approving SEC filings/disclosures



Director's Legal Duties – Types

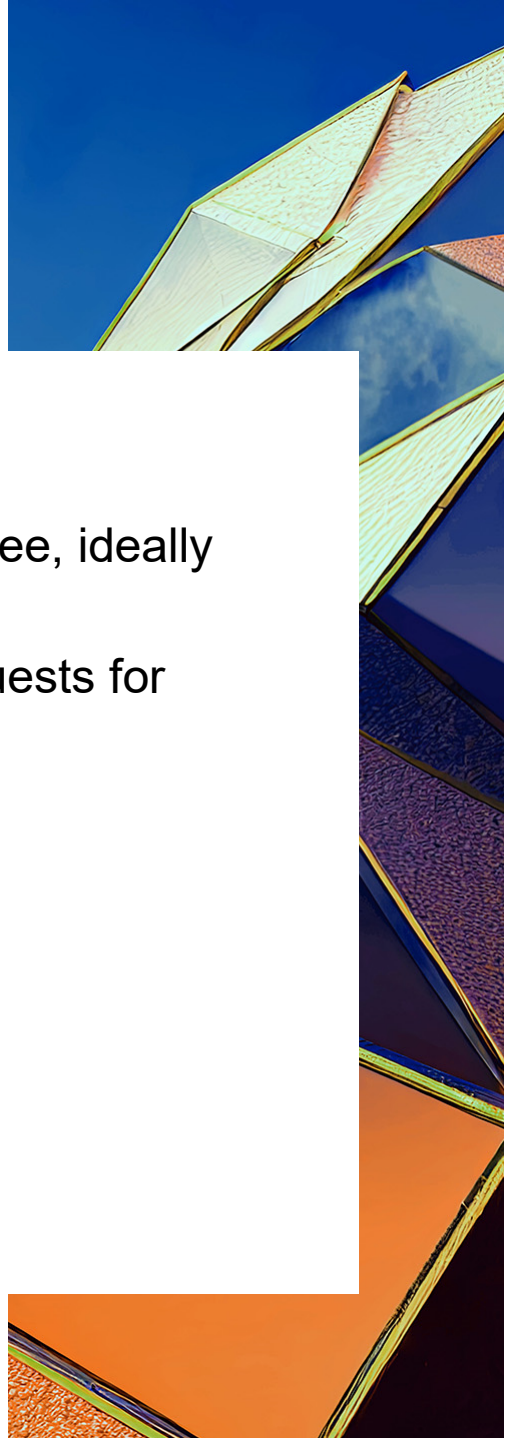
- **<u>Director Fiduciary Obligations:</u>**
  1. **Duty of Care**
     - Directors must act on an informed basis, in good faith and with the care that an ordinary prudent person in a like position would exercise
  2. **Duty of Loyalty**
     - Directors should not use their corporate position to make a personal profit or gain or for other personal advantage
  3. **Duty to Supervise (Oversight)**



Best Practices to Help Satisfy Director's Duty of Care

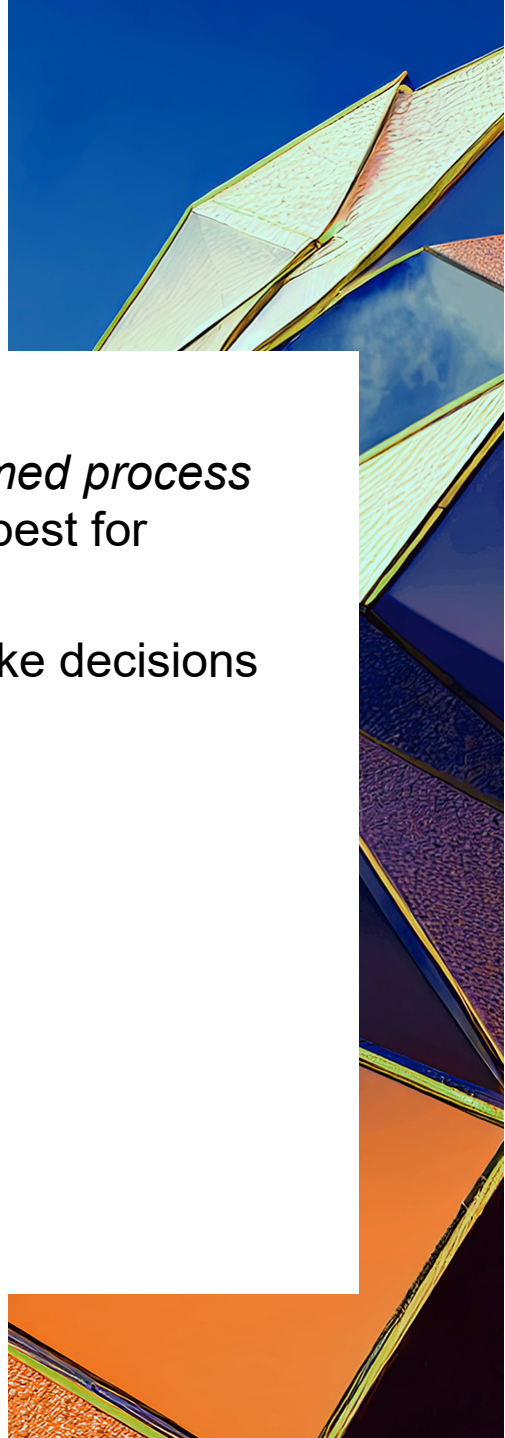
- Document decision-making and corporate approval process carefully in **Board minutes**
  - Balance between no record of deliberations and keeping transcripts
  - Must be more than a mark-up of last meeting's minutes
  - Reflect substance and process of meeting; **emphasis on factors and reference to policies *considered by Board* when reaching decisions**
- Get draft minutes out quickly for review by all directors
- Consider how record will look to future audiences (media, court) when sending out advance Board books

Best Practices to Help Satisfy Director's Duty of Care (cont.)



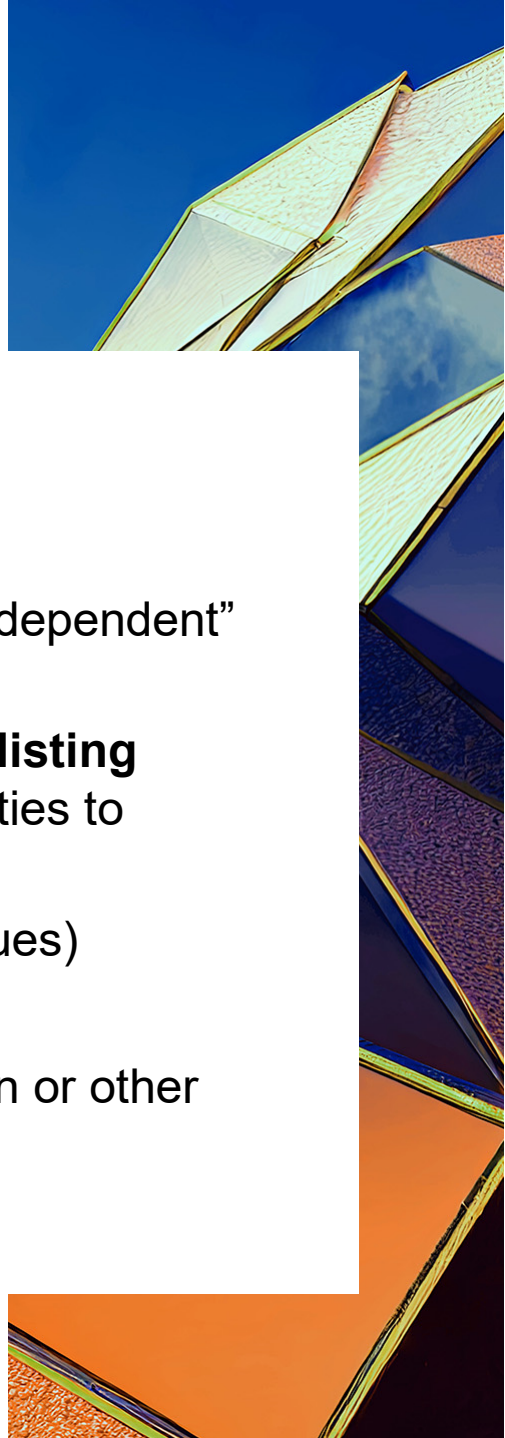
- Hire independent experts, advisors or consultants who report to Board
  - Expert's work product and advice should be delivered directly to the Board or committee, ideally in-person at Board meetings
- Effective follow-up on open issues and director requests should occur–questions or requests for information should not remain unanswered
- Board and its committees should follow their own charters and governance guidelines
- [*New*] Consideration of constituencies other than shareholders
  - More courts now allowing/requiring consideration of more stakeholders

Duty of Care – Business Judgment Rule



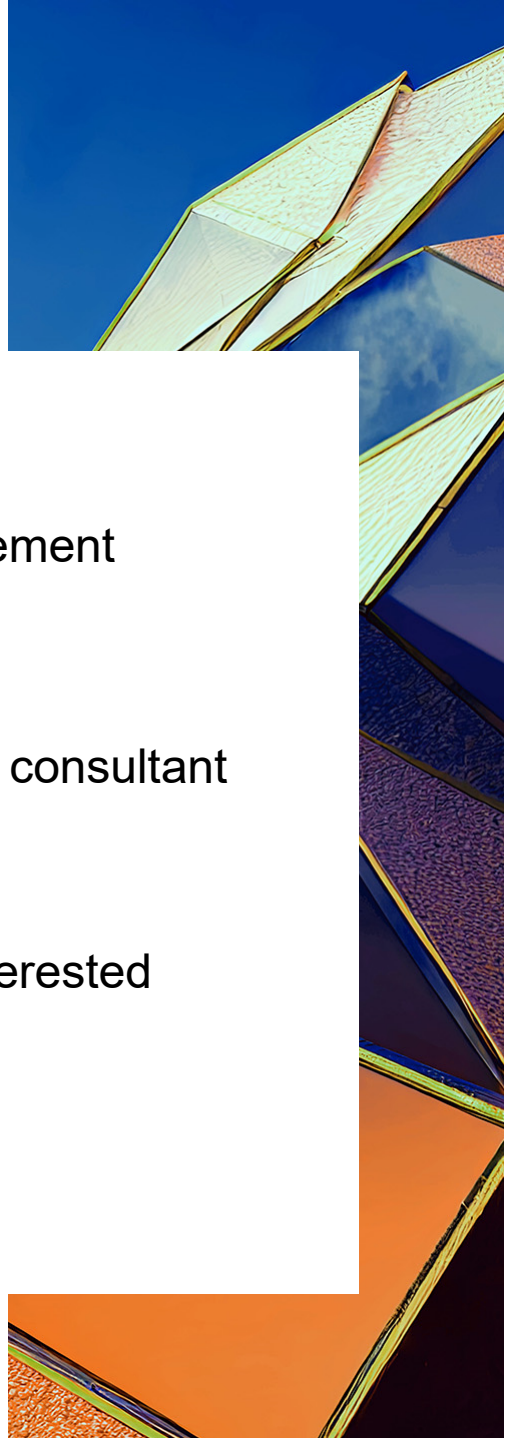
- BJR Standard: Business decisions made by *disinterested directors pursuant to an informed process are legally presumed* to be made on informed basis and in honest belief the decision is best for company, even if the decision turns out to be unwise or unsuccessful
- Legal system will judge directors and the company on the *process* the Board took to make decisions
- BJR protection:
  - Shields directors from personal liability
  - Allows directors to be indemnified and qualify for D&O insurance coverage
  - Enables courts to dismiss meritless shareholder suits at the beginning of a lawsuit
  - Does BJR protection extend to *officers?* Split of authority

Duty of Loyalty – Overview



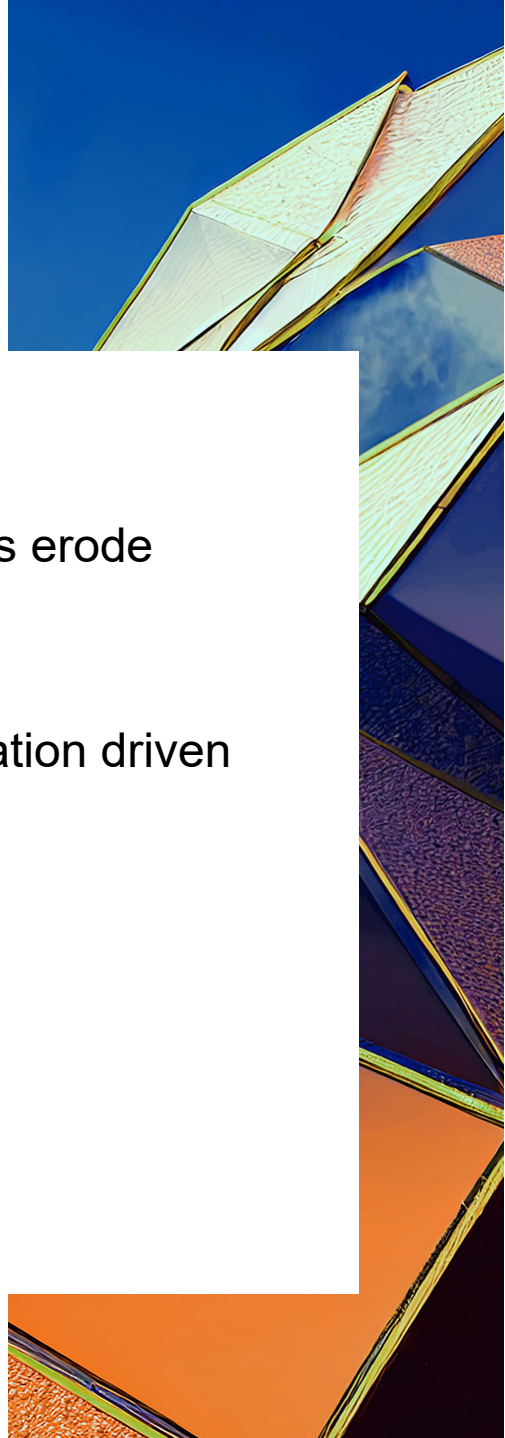
- ***BJR is Unavailable to Conflicted Directors:***
  - **Director Independence/No Conflict of Interests**
    - Director must not only be “independent” from management/corporation, but also “independent” from the transaction/people at issue
    - **Independence is judged far more rigorously in litigation than NASDAQ/NYSE listing standards!** Can include social relationships, business relationships, other informal ties to management/other directors and to the transaction at issue
    - “Personal” interest need not be financial; can be reputational (*e.g.*, employment issues)
  - **Corporate Opportunity**
    - Directors should not use their position within the company for personal financial gain or other personal advantage

Best Practices to Help Satisfy Director's Duty of Loyalty



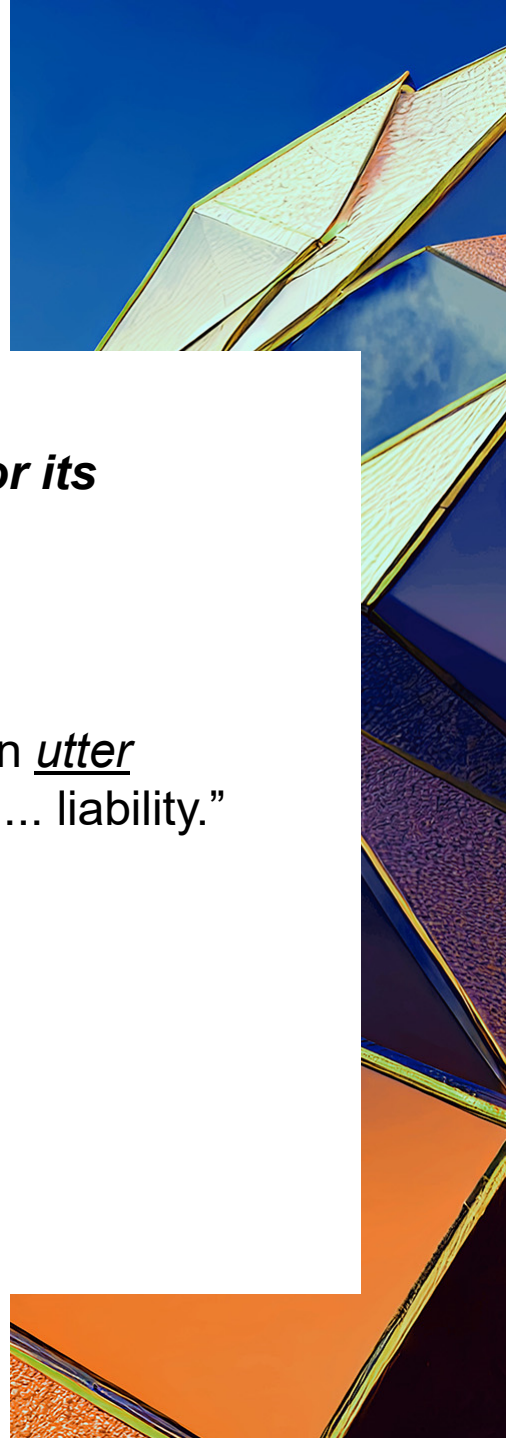
- Revisit and refine director independence criteria
  - Consider all financial/social ties between directors and between directors and management
  - Understand conflicting obligations of directors (other boards, full-time jobs, etc.)
  - Annual Board questionnaire is important
  - Board pay usually does not create conflict, but if levels are high, obtain compensation consultant input
  - Also, focus on conflicts of financial/legal advisors
- Expect full disclosure and scrutiny of all conflict of interest situations; approved by disinterested directors after full financial analysis
- Actively enforce company's code of conduct

Recent Trends – Role of Board



1. **Heightened Supervisory Role**
   - Shift to more active management role (The New Paradigm) as protections for directors erode under new duty to supervise standard
2. **Increasing Focus on ESG Factors**
   - Board's focus goes beyond short-term financial gain and looks at long-term value creation driven by additional factors such as societal contribution
3. **Multi-Stakeholder Approach**
   - Broader view of stakeholders (beyond shareholders)

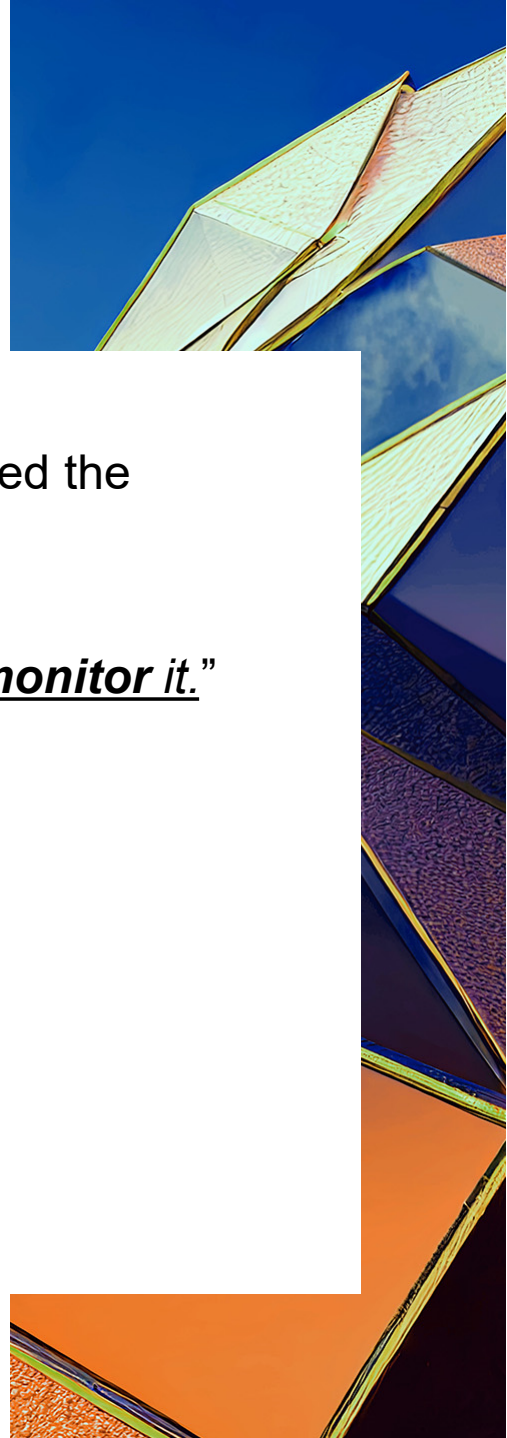
Duty to Supervise – Overview



Boards have an *affirmative duty* to implement a reporting and controls system ***and monitor its functioning***

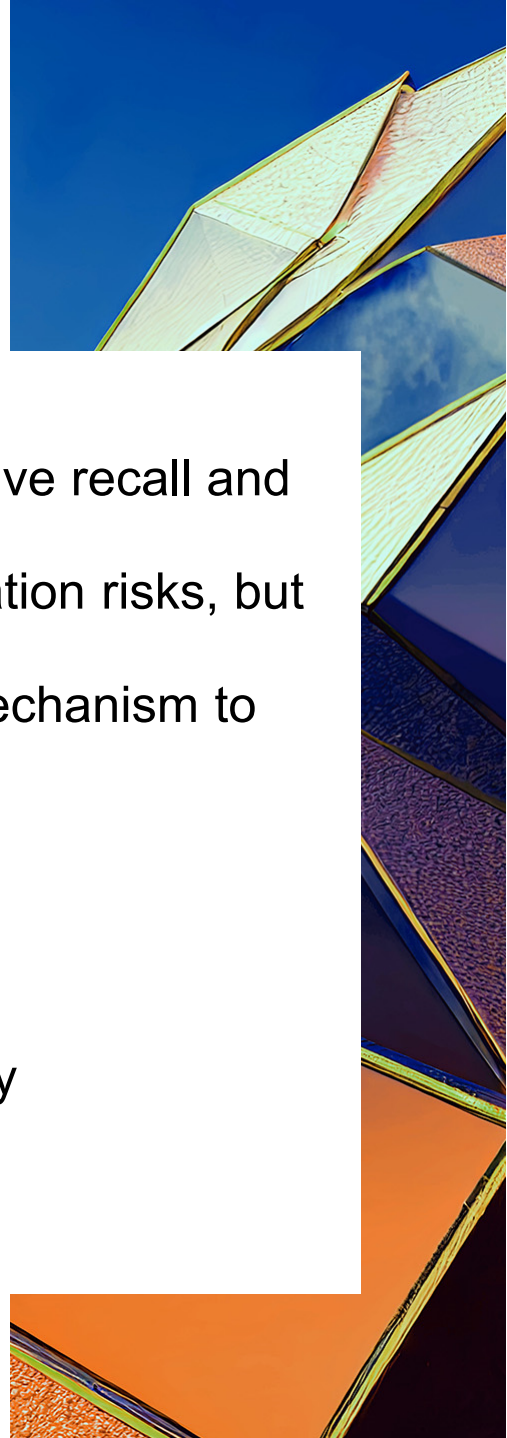
- Prior to 2017, very few successful "failure to supervise" cases
- **Pre-2017 Standard:**
  - "Only a *sustained or systematic failure* of the board to exercise oversight – such as an *utter failure to assure a reasonable information and reporting system exists* – will establish ... liability." *In re Caremark Int'l,* 698 A.2d 959, 967 (Del. Ch. 1996)

Duty to Supervise – Overview (cont.)



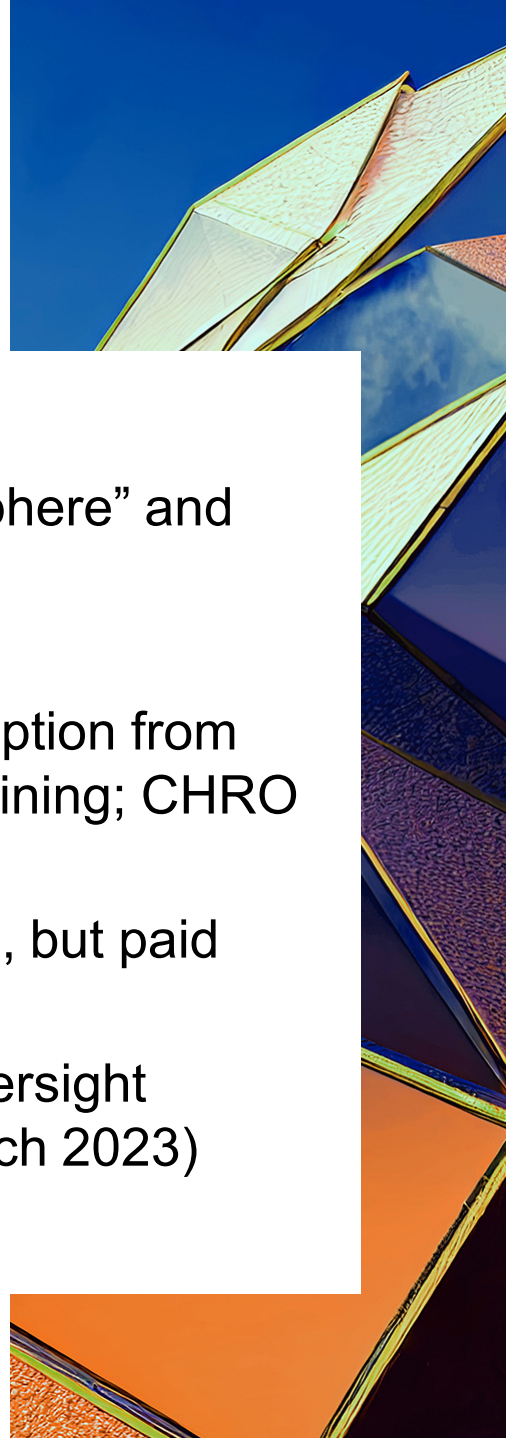
- Recent DE cases — especially *Marchand v Barnhill,* 212 A.3d 805 (Del. 2019) — changed the protective *Caremark* standard
- **Standard now:**
  - Directors "*must make a good faith effort to implement an oversight system and then **monitor** it.*"
  - Not just required by the Courts; Regulators require it, too:
    - SEC: *Seaboard* standards
    - DOJ: https://www.justice.gov/criminal-fraud/page/file/937501/download

Trend #1 – Heightened Supervisory Role



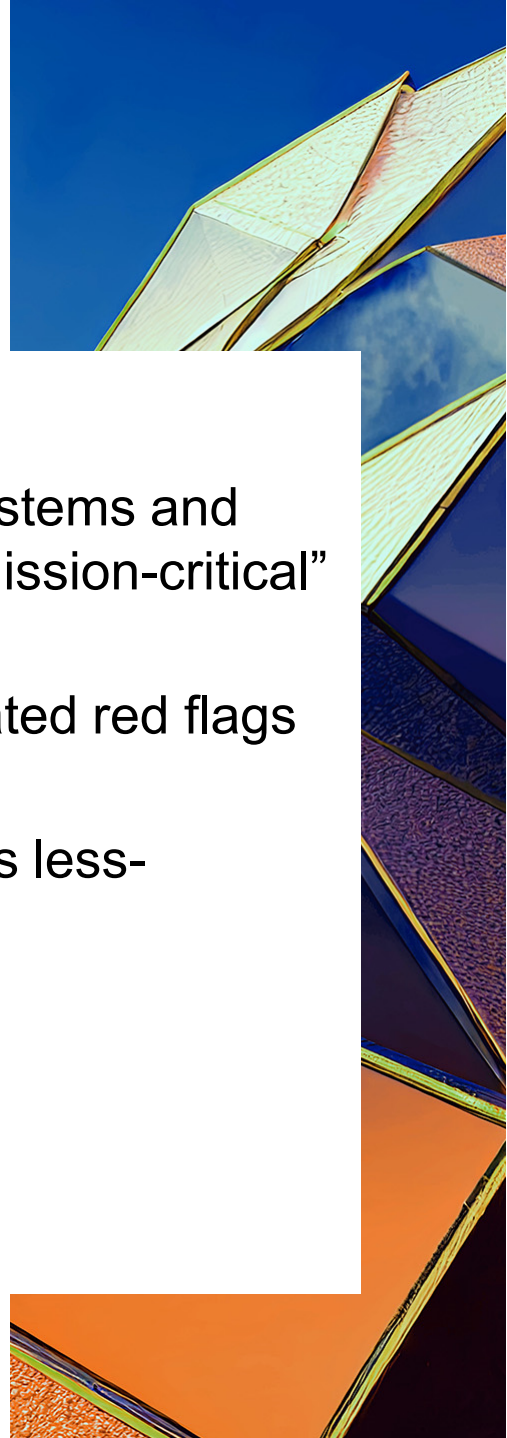
- ***Marchand* Facts**:
  - Blue Bell Creameries suffered deadly listeria outbreak; 3 consumers died. Massive recall and layoffs ensued. To stay afloat, new financing obtained, but under negative terms
  - Management knew of inspection reports raising major concerns about contamination risks, but didn't tell Board
    - Board failed to ensure effective food safety compliance system, and had no mechanism to ensure material food safety issues would be flagged at the Board level
    - No board Risk Committee
    - Board delegated to management public reaction to crisis
  - Held:
    - Chancery Court initially dismissed claims under *Caremark*
    - Delaware Supreme Court *reversed,* and allowed claims to proceed to discovery

Trend #1 – Heightened Supervisory Role



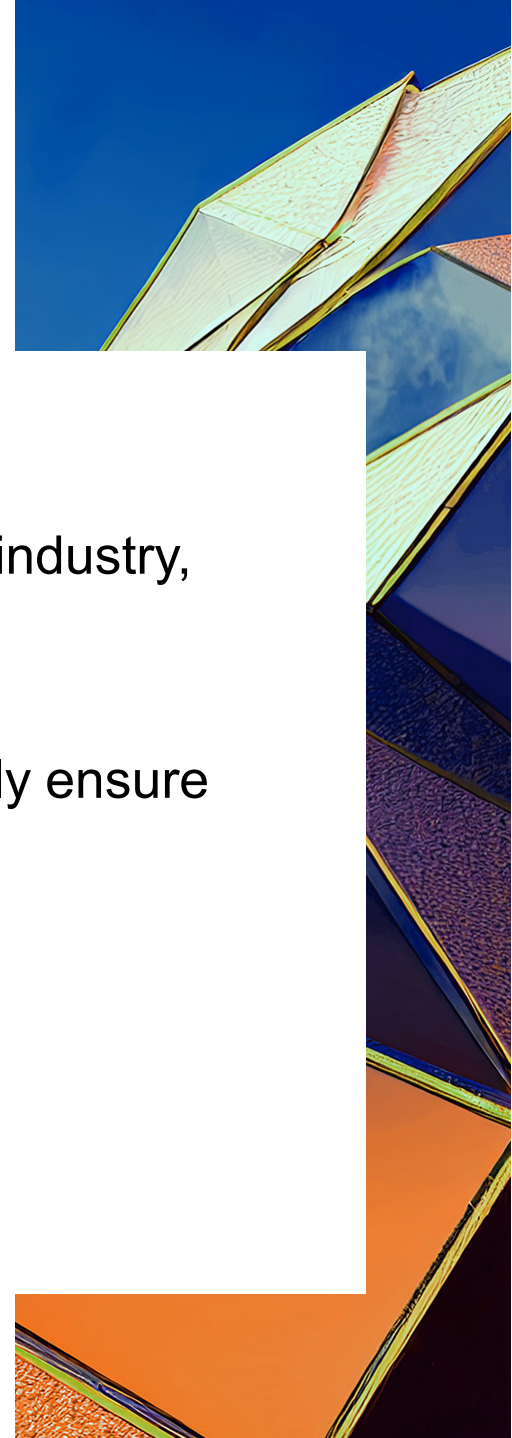
- **Extension of *Marchand* to Corporate *Officers* --** *In re McDonald's*
  - After CEO hired, he in turn hired CHRO who allegedly fostered "party atmosphere" and also personally allegedly sexually harassed and assaulted employees
  - In 2016 and 2018, company-wide employee walkout in over 30 US cities
  - 2018: Board learned of allegations against CHRO; CEO recommended exception from "zero tolerance" policy. Board keeps CHRO but hires consultant, requires training; CHRO continues to violate policy; Board fires him for cause
  - 2019: Board fires CEO for having sexual relations with multiple subordinates, but paid $40MM+ severance upon ouster
  - Held: *Caremark* claims against CHRO not dismissed; CHRO also held to oversight fiduciary duties (Jan. 2023). *Caremark* claims against Board dismissed (March 2023)

Trend #1 – Heightened Supervisory Role



- **2-Pronged Compliance Oversight Test Adopted in *McDonald's***
  - 1st Prong: "Information System Claims," where Board lacks information systems and controls designed to provide timely information to address "essential and mission-critical" legal compliance
  - 2nd Prong: "Red-Flags Claims," where Board's information systems generated red flags indicating wrongdoing" but failed to respond
    - Note distinction between *legal* "red flags" and *business* "red flags": courts less-forgiving when *legal* red flags are ignored
- Other Issues:
  - How to document compliance with *officer* fiduciary duties?
  - Will BJR protection be extended to officers?

Trend #1 – Heightened Supervisory Role



- **Boards will now be asking Management**:
  - **What are the "mission-critical" risks** facing our company, considering our industry, our scope of operations, and our mix of products?
    - Note: cultural factors like sexual harassment can be "mission-critical"
  - **What key metrics** do we need to hear about from management to reasonably ensure these risks are being addressed?

Trend #2 – Increasing Focus on ESG

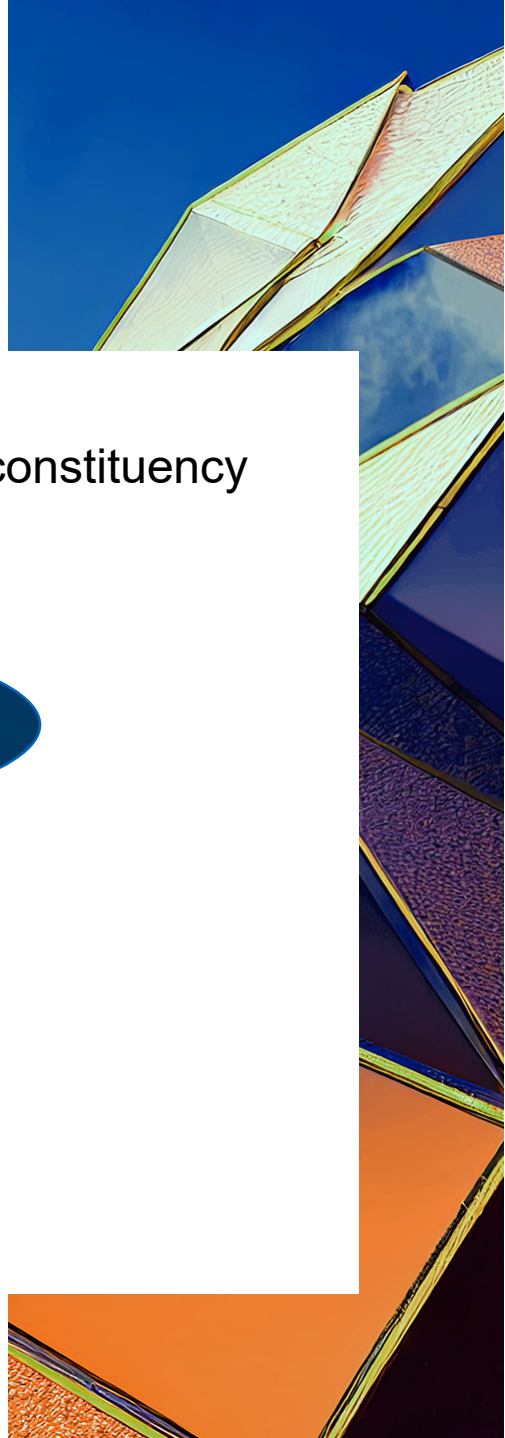
- Environmental, social, and governance (ESG) investing
- **What are ESG Disclosures?**
  - Disclosures on environmental, societal, and governance factors made by public companies to help investors understand risks to the company's financial performance or other issues, such as the impact of the company's business on communities

Table 1: Examples of Environmental, Social, and Governance Factors

Environmental	Social	Governance
Climate change impacts and greenhouse gas emissions	Labor standards	Board composition
Energy efficiency	Human rights	Executive compensation
Renewable energy	Employee engagement	Audit committee structure
Air, water, resource depletion, or pollution	Customer satisfaction	Bribery and corruption
Waste management	Community relations	Whistleblower programs
Biodiversity impacts	Gender and diversity	Accident and safety management

Source: GAO analysis of documentation from the CFA Institute, Sustainable Accounting Standards Board, and Principles for Responsible Investment. | GAO-20-530

Trend #3 – Multi-Stakeholder Approach

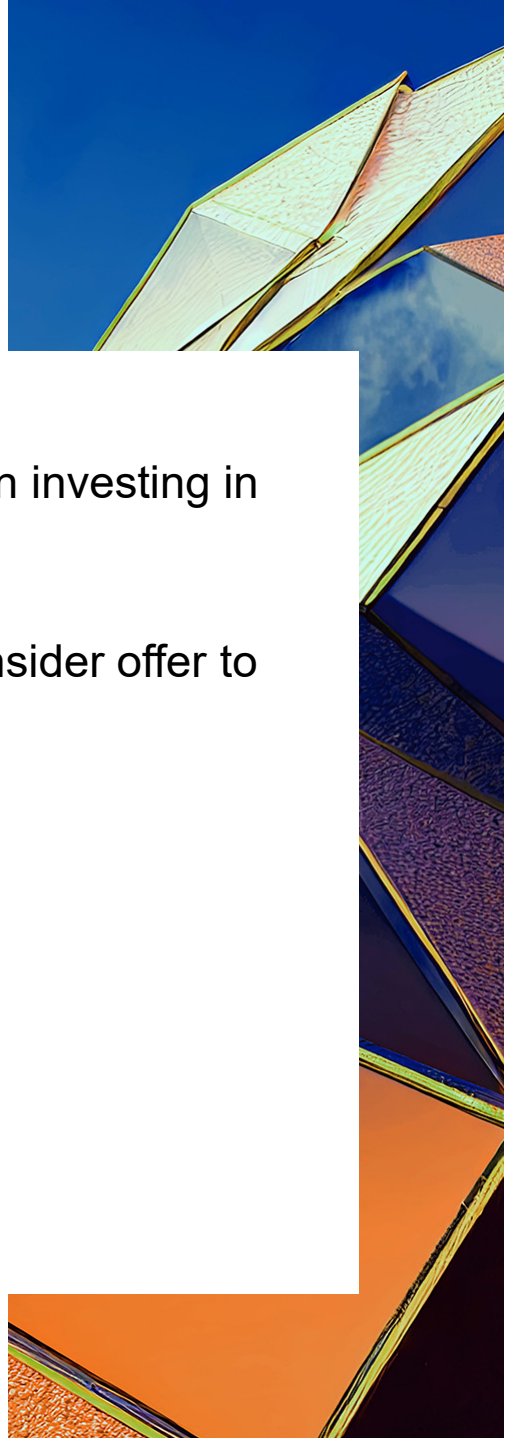


- In 2019, 181 large-company CEOs joined the Business Roundtable in adopting a multi-constituency approach:

> "While each of our individual companies serves its own corporate purpose, ***we share a fundamental commitment to all of our stakeholders***"

- "Stakeholders" include **investors, employees, communities, suppliers, customers**
- Legislative adoption:
  - Many states (other than DE) have multi-stakeholder *statutes*
  - Query whether DE will eventually adopt similar approach

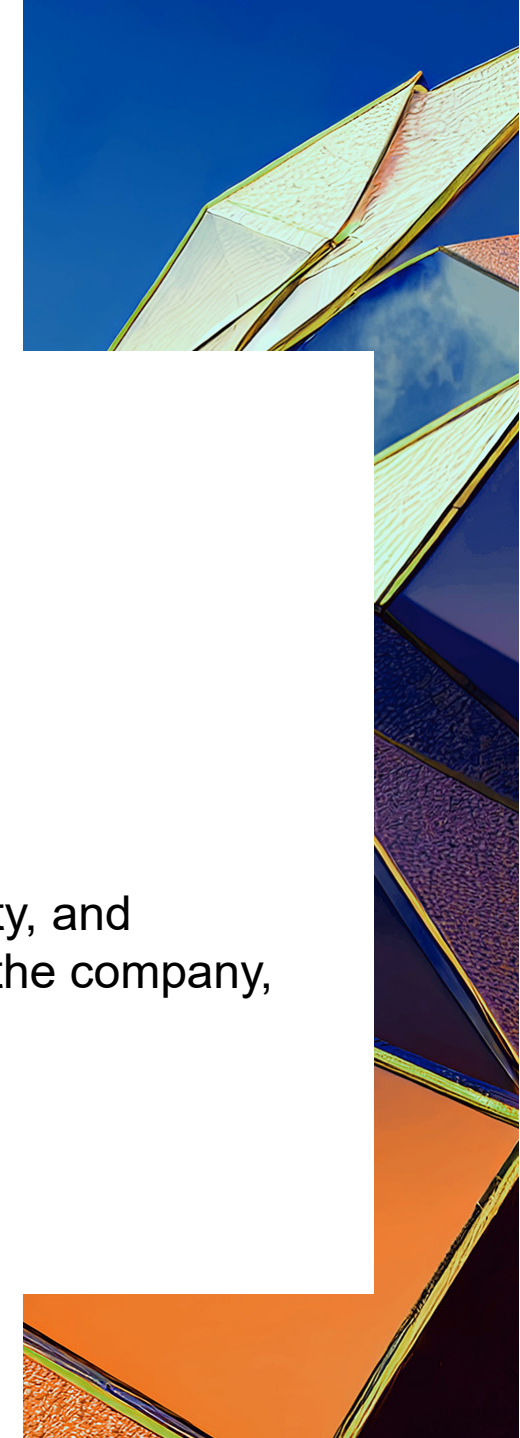
Trend #3 – Multi-Stakeholder Approach



Case Study – Twitter

- April 2022: Elon Musk offers $54.20/share – a 54% premium over the day before he began investing in Twitter and a 38% premium over the then-trading price -- with $1B+ break-up fee
- BUT: significant customer/employee pushback on offer
- Twitter incorporated in Delaware/subject to *Revlon* rule, *i.e.,* once the board decides to consider offer to buy all/substantially all the company, duty shifts to maximize return to shareholders
- Board accepts Musk offer:
  - Musk attempts to back out of deal, but MAC clause prohibitive
  - Musk arrives as CEO – while also concurrently CEO of Tesla, SpaceX
  - Mass exodus of senior management; eventual mass exodus of technical staff
  - Controversy over new content-policing policy; customers/advertisers leave
- ***Would result have been different in a multi-stakeholder jurisdiction???***

Board Duties in the Time of Social Unrest



- Heightened sensitivity about social, cultural factors
  - Enormous impact on the company's reputation
  - People want to see companies do the right thing, not just say they will
  - But Board needs to be strategic about which social issues they weigh in on
- High demand for chief diversity, equity, and inclusion (DE&I) officers
  - Ensure DE&I officer has an active role & seat at the table
  - Work with DE&I officer to examine company's performance in terms of diversity, equity, and inclusion, with a real discussion about hiring practices, representation at all levels of the company, and pay equity

Board Duties in the Time of Social Media/Unrest

CVS pharmacy®

CVSquitsforgood

"Walgreens Faces Blowback for Not Offering Abortion Pill in 21 States"

Walgreens

BLACK COMMUNITY COMMITMENT

DELTA

Coca-Cola

Directors Sued Under New Standards

- Boeing – $237MM for failure to oversee development of 737Max jets; board separately sued i/c/w $23MM payout to ousted CEO for #MeToo issues
- Fox News, Wynn Resorts – $90MM and $41MM settlements of derivative claims over #MeToo issues
- Google – derivative suits from $90MM payout to one ousted exec, $45MM for another
- McDonald's – $70MM payout for ousted CEO
- 10+ derivative suits (and counting) for failure to diversify board
- However…may be seeing a shift away: WeWork's ousted CEO denied $185MM payout
- Bottom Line: ***Review "For Cause" Termination Clauses in Key Exec Employment Agreements!*** Also note new SEC "clawback" rules for financial restatements.

Board's Response to Management in Trouble

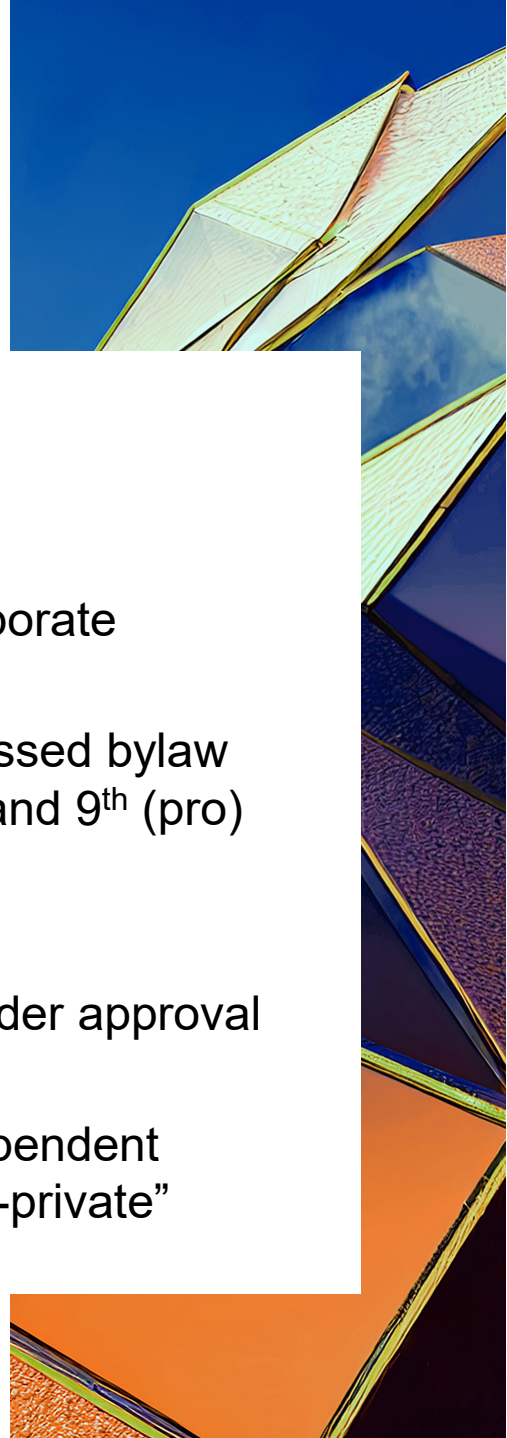
Before: "We stand behind our CEO/Management"

Board's Response to Management in Trouble (cont.)

Now: "We're going to get to the bottom of this"*

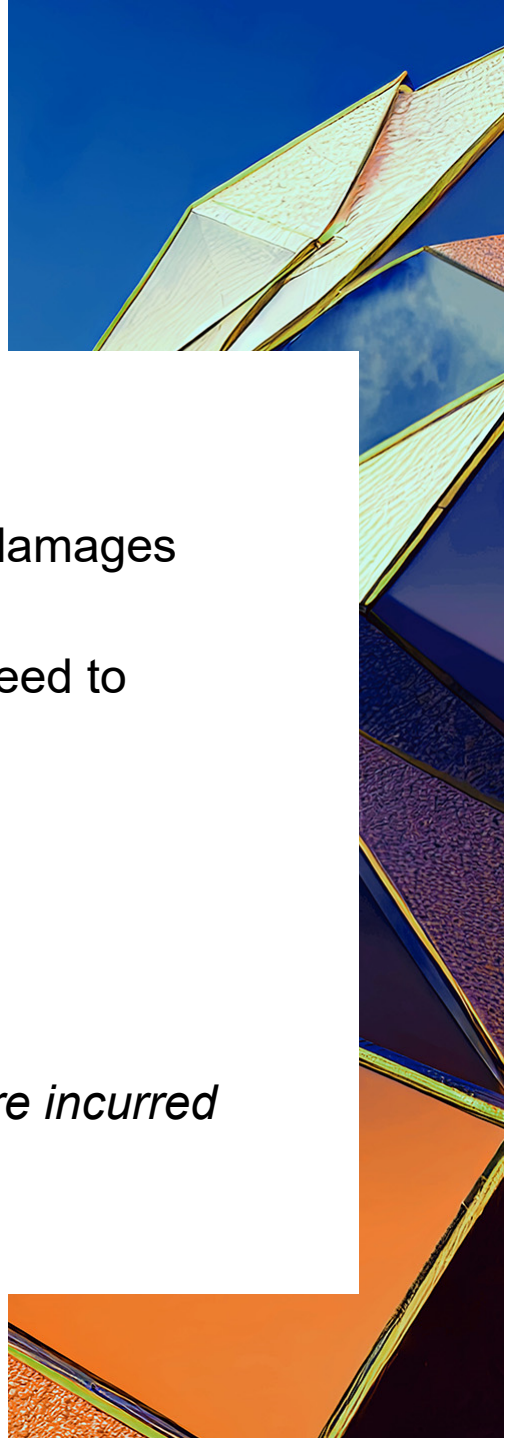
*And using our own advisors, thank you.

Other Issues on the Horizon



- Super-Voting Stock Agreements – Delaware courts apply BJR, and will typically uphold
- Viability of Forum Selection Clauses
  - Under 8 Del. C. 115 (2015), DE corporations can adopt bylaws requiring "internal corporate claims" to be brought solely in Delaware courts
    - What about federal securities law claims? *Sciabacucchi v. Salzberg* (Del. 2020) blessed bylaw limitations requiring venue for '33 Act claims in federal DE court; but note 7th (con) and 9th (pro) Circuit split re: viability of FSCs for *derivative* securities law claims.
- Challenges to Contractual Stockholder Consent Rights
  - Shareholder challenges contending Board abdicates its duties by giving one shareholder approval over, *e.g.*, CEO selection/termination
- Extension of *MFW* conflicted shareholder framework (i.e., transaction approved by independent Special Committee and "majority of the minority" vote of shareholders) outside of "going-private" context. *E.g.*, *Match Group* (reverse spin-off), etc.

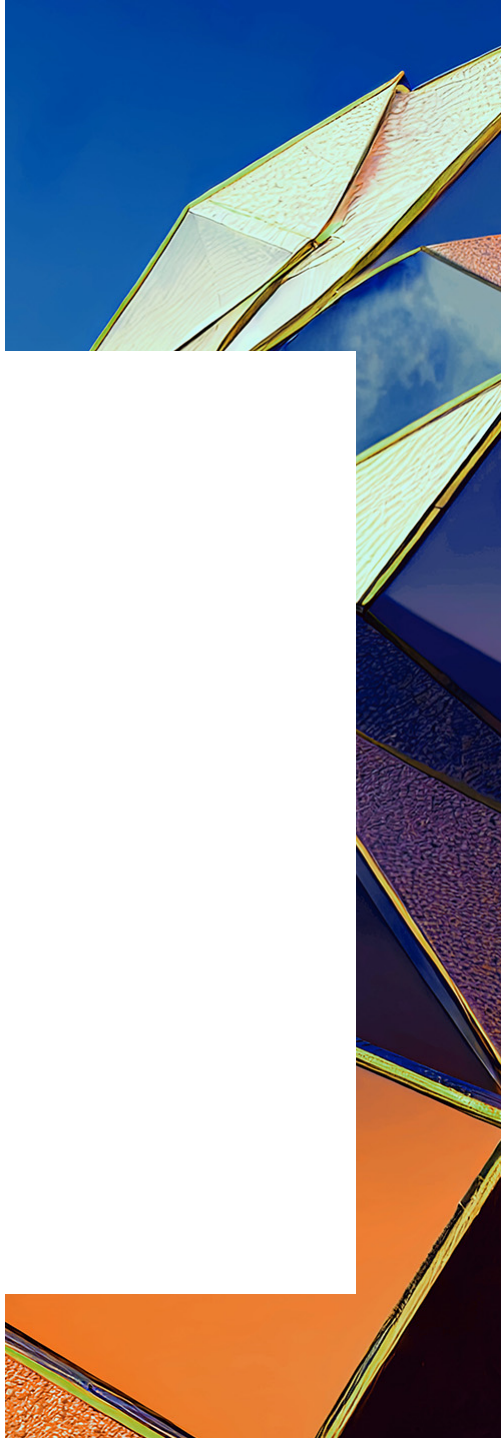
Key Protections: *Exculpatory and Indemnity Clauses*



1. **Exculpatory Clause**
   - DE 102(b)(7) in corporate charters – limits personal liability of directors for monetary damages (but not injunctive relief)
   - Statutory protections now extended to Delaware *officers* since August 2022, though need to include in charter to have protection

2. **Indemnification Provisions**
   - Ensure you have state-of-the-art corporate indemnification provisions
     - Explore expanded bylaws or individual agreements
     - Indemnification provisions should also include *advancement of legal fees as they are incurred*
     - Certain states have expansive statutory protections

Indemnification and Liability Shields: *D&O Insurance, Forum Selection Clauses*

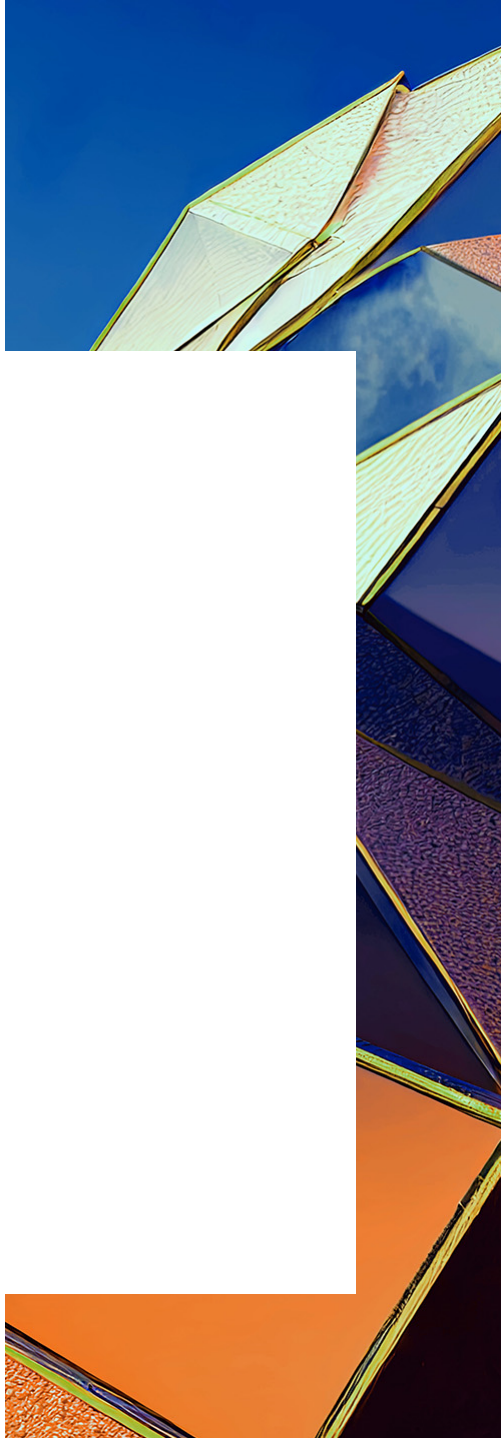


3. **<u>D&O Policy Protections</u>**
   - D&O policies are *not* "One Size Fits All": *they are negotiable!*
     - Definition of "Claim": formal litigation or investigation? Or something else?
     - "Bump-up" Provisions
     - Ability to Select Counsel of Choice
     - Retention vs. Policy Limits; Coverage of Individual, vs. Company
   - This requires expert advice!

4. **<u>Forum Selection Clauses</u>**

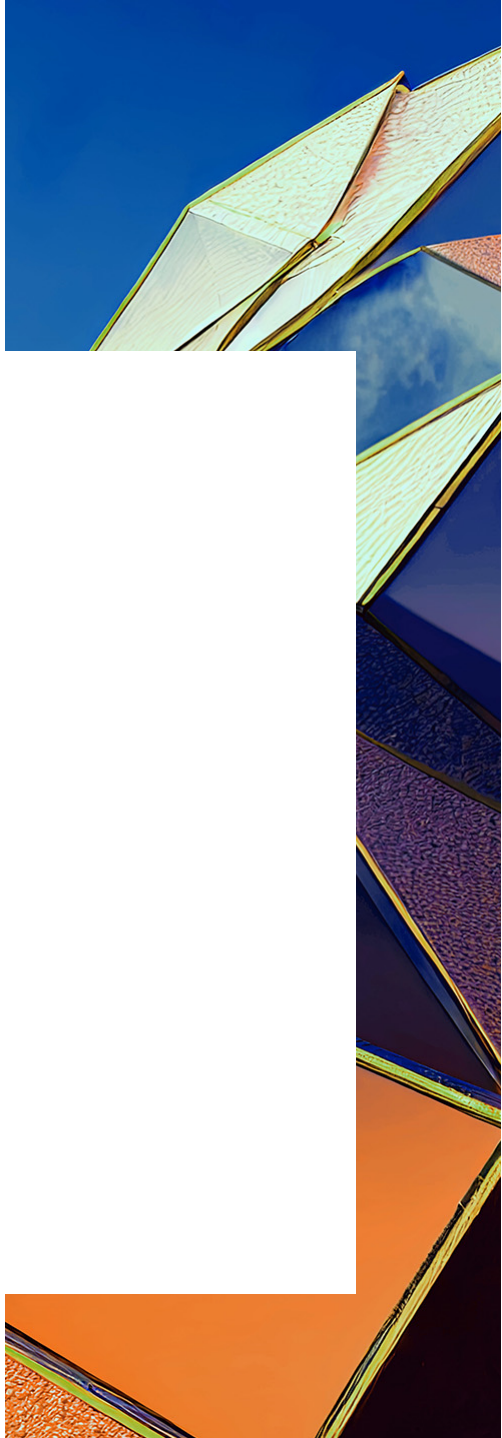
Thank You

- Questions?



About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 25 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.



FOLEY
FOLEY & LARDNER LLP

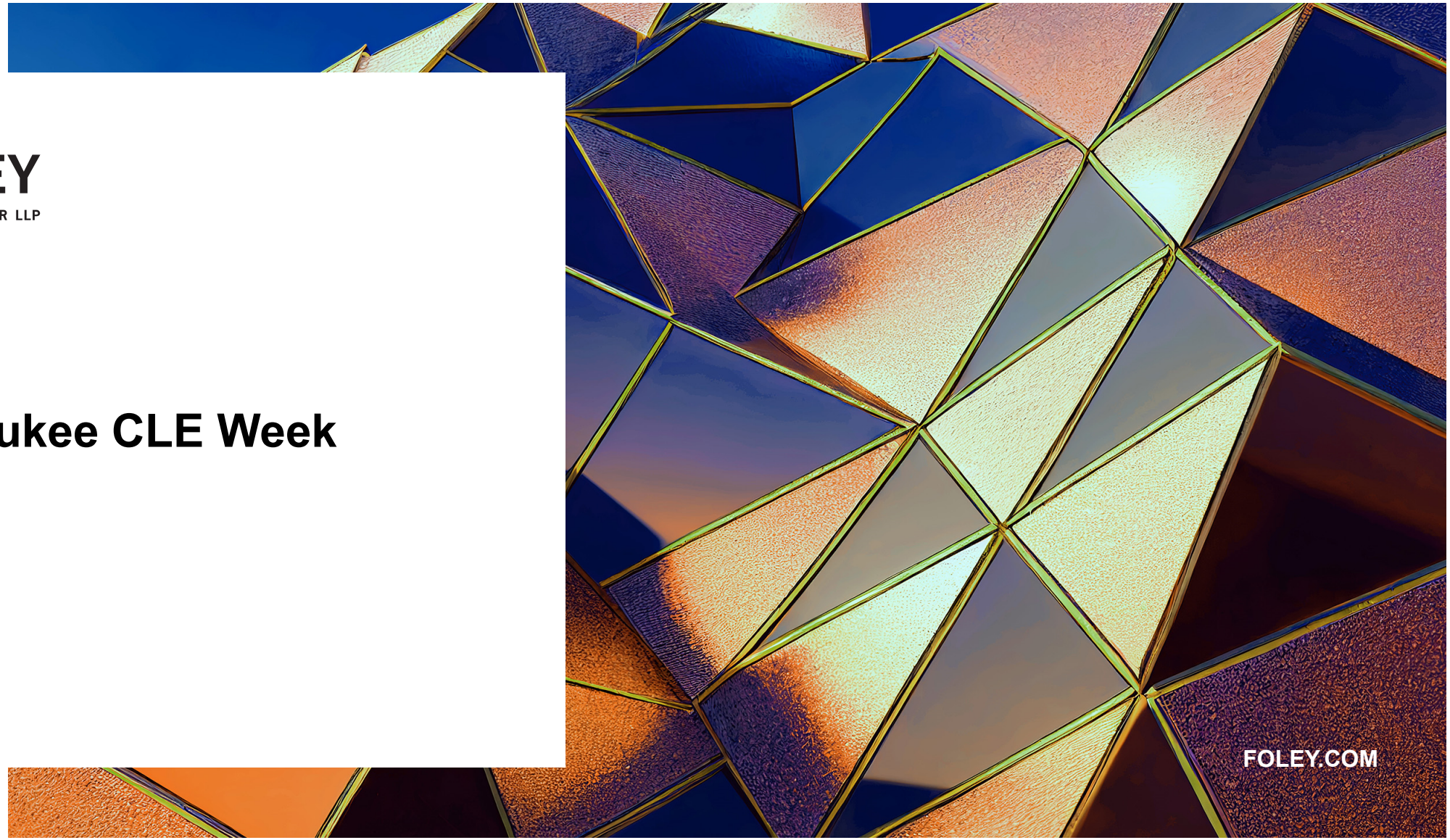
FOLEY.COM

FOLEY

FOLEY & LARDNER LLP

Milwaukee CLE Week

December 7, 2023



Thank You

- Presentation materials can be downloaded from www.foley.com/milwaukeecleweek2023
- Return your completed CLE form and survey to the registration station
- Register for Virtual CLE Week using the QR code at the bottom of today's agenda