Skadden

The Informed Board

Summer 2024

Across industries, companies are facing new and uncertain regulatory pressures and demands in areas including artificial intelligence, sustainability, algorithmic pricing and fintech-bank relations. In this issue of *The Informed Board* we discuss what boards need to ask and understand about these issues, as well as ways for companies to mitigate risks and establish appropriate governance procedures.

In addition, in our latest podcast, we discuss how and what companies can communicate to investors about the internal working of their boards, and what makes them effective.

AI Safety: The Role of the Board in Assessing and Managing AI Risk

- As AI systems become more complex, companies are increasingly exposed to reputational, financial and legal risk from developing and deploying AI systems that do not function as intended or that yield problematic outcomes. The range of potential risks is wide and can include fostering discriminatory practices, causing products to fail, and generating false, misleading or harmful content.
- The risks of AI, and the legal and regulatory obligations, differ across industries, and depending on whether the company is the developer of an AI system or the entity that deploys it — a line that may be difficult to draw.
- Boards must navigate a quickly evolving regulatory environment that does not always offer consistent approaches or guidance.

Key AI Safety Risks: People, Organizations, Supply Chains and Ecosystems

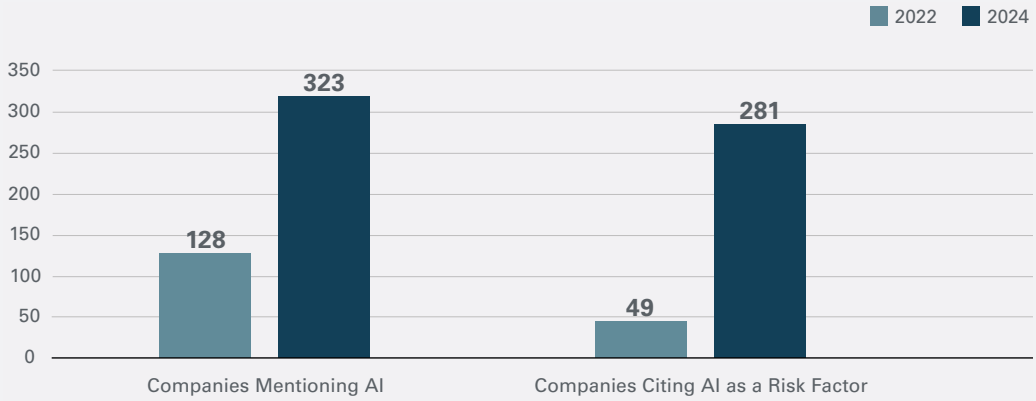
The National Institute of Standards and Technology (NIST), a Department of Commerce agency leading the U.S. government's AI risk management approach, suggests that AI risk be evaluated at three levels of potential harm:

- **Harm to people** (*i.e.*, harm to an individual's civil liberties, rights, physical or psychological safety or economic opportunity), such as deploying an AI-based hiring tool that perpetuates discriminatory biases from past data.
- **Harm to organizations** (*i.e.*, harm to an organization's reputation and business operations), such as using an AI tool that generates erroneous financial reports that were not properly reviewed by humans before being publicly disseminated.
- **Harm to ecosystems** (*i.e.*, harm to the global financial system or supply chain), such as deploying an AI-based supply management tool that functions improperly and causes systemic supply chain issues that extend far beyond the company that deployed it.

Companies may be subject to some or all of these AI safety risks, which often overlap.

Boards should be informed about the developments and deployment of AI systems within their companies, the AI regulatory landscape to which their companies are subject, and the benefits and risks of each use of an AI system. Boards should also reassess AI systems that may have been in use at the company for a number of years, in light of the increased focus by regulators and the general public.

All Mentions of AI in S&P 500 10Ks



Source: Arize AI

The Current AI Regulatory Landscape

United States

To date, the U.S. has not enacted any omnibus AI legislation, and there is none on the immediate horizon. Instead, the federal government has issued a series of reports, general guidance, and frameworks emanating from an October 2023 AI Executive Order (EO). A July 2024 statement from the White House provides a useful summary of these reports and frameworks.

Of most relevance to boards is a suite of AI risk management tools published by NIST. This includes an AI Risk Management Framework, guidelines on Managing Misuse Risk for Dual-Use Foundation Models and a Risk Management Profile on Generative AI. A complete list of NIST statements and publications on AI can be found at the NIST Trustworthy and Responsible AI Resource Center.

While there is no omnibus federal AI law, federal agencies and regulators have made clear that existing laws apply equally to AI systems. For example, the Federal Trade Commission has brought a number of actions and made a number of statements regarding AI deployments based on its authority to protect against "unfair or deceptive acts or practices."

Boards also need to be cognizant of a growing number of state-specific AI laws. For example, Utah enacted the Utah Artificial Intelligence Policy Act, which imposes disclosure requirements on entities using generative AI tools for customer interactions. The law went into effect in May 2024.

Also in May 2024, Colorado enacted the Colorado Artificial Intelligence Act, which is designed to protect against algorithmic discrimination and imposes various disclosure and risk assessment obligations on companies developing or deploying AI systems that make "consequential decisions" involving areas such as financial services, health, and education. The law will go into effect on February 1, 2026.

European Union and United Kingdom

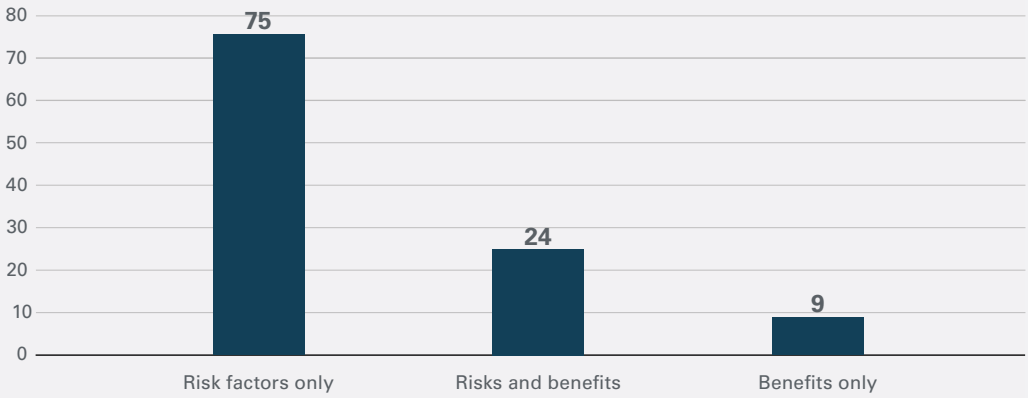
The EU has taken a more direct and risk-based approach to AI regulation than the United States. The EU's landmark AI Act — which came into force on August 1, 2024, and will be fully effective from August 2, 2026 — governs all AI models marketed or used within the EU. The law creates four tiers of AI systems based on the risk they present: unacceptable (which are prohibited), high, limited and minimal. The risk categories carry with them various risk assessment, disclosure and governance obligations.

While these categories and the specific compliance requirement will be further clarified through guidance, boards whose companies are, or may be, marketing or using AI models in the EU should stay informed about the EU AI Act and their organizations' approach to compliance.

In addition, European privacy regulators have already stepped in to use existing privacy laws to block the roll-out of generative AI products in Europe, and have launched court actions against companies that seek to develop AI models without approval from privacy regulators.

While the U.K. does not yet have any laws that mirror the EU AI Act, the new Labour government recently announced its intention to develop AI safety legislation, and its privacy regulator, the Information Commissioner's Office, has launched enforcement actions against AI companies that fail to complete risk assessments before deploying AI-powered products.

Generative AI Mentions in S&P 500 10Ks (2024)



Source: Arize AI

Guiding Principles for AI Corporate Governance

In general, there are several guiding principles boards should keep in mind to effectively navigate AI corporate governance and manage AI safety risk.

- **Understand the company's AI risk profile.** Boards should have a solid understanding of how AI is developed and deployed in their companies. Taking stock of a company's risk profile can help boards identify the unique safety risks that AI tools may pose.
- **Be informed about the company's risk assessment approach.** Boards should ask management whether an AI tool has been tested for safety, accuracy and fairness before deployment, and what role human oversight and human decision-making making play in its use. Where the level of risk is high, boards should ask whether an AI system is the best approach, notwithstanding the benefits it may offer.
- **Ensure the company has an AI governance framework.** The board should ensure that the company has such a framework to manage AI risk, and then reviews it periodically to make sure it is being properly implemented and monitored, and to determine the role the board should have in this process.
- **Conduct regular reviews.** Given the rapid pace of technological and regulatory developments in the AI space, and the ongoing discovery of new risks from deploying AI, the board should consider implementing regular reviews of the company's approach to AI, including whether new risks have been identified and how they are being addressed.
- **Stay informed about sector-specific risks and regulations.** Given how quickly the technology and its uses are evolving, boards should stay informed about sector-specific risks and regulations in their industry.

Authors

Ken D. Kumayama / Palo Alto
Stuart D. Levi / New York
William E. Ridgway / Chicago
David A. Simon / Washington, D.C.
Nicola Kerr-Shaw / London
Susanne Werry / Frankfurt
Jacob F. Bell / Washington, D.C.

Are Fintechs Prepared for More Regulatory Scrutiny? Questions Fintech Boards Will Want To Ask

- The 2024 elections may usher in laws and regulations that impact fintechs, making it important for management to identify the areas that present the greatest challenges and opportunities.
- As fintechs grow, they should consider whether they have all necessary licenses to operate and whether existing compliance and risk management infrastructure should be augmented to be "fit for purpose."
- Bank-fintech partnerships are under the regulatory microscope. Fintechs that rely on bank partners should evaluate how their business models could be affected if partnerships are terminated or no longer available on existing terms.
- Reliance on a few counterparties and providers raises concentration risk and operational resiliency issues. Fintechs should prioritize the development and regular testing of contingency plans.

As summer winds down and the year-end comes closer in sight, boards of financial technology firms should take stock of where they are on four key areas:

- Legislative and regulatory change.
- Licensing and compliance risks.
- Bank-fintech partnership scrutiny.
- Concentration risks and operational resiliency issues.

Boards should expect that increasing interest in the fintech sector by U.S. financial regulators will spark questions — not least of all from investors — on how these areas are being addressed.

Preparing for Legislative and Regulatory Change

One of the most significant developments in financial services in the last 10 years has been the role of non-bank firms operating outside the traditional bank regulatory perimeter providing core banking and other financial services. As the fintech sector's market share and prominence has grown, so too has the regulatory scrutiny over its various participants. The ability to anticipate and respond to regulatory change is — and will be — a distinguishing characteristic of fintechs with the most viable and successful business models.

Global regulators are increasingly concerned about the linkages between the traditional banking sector and non-bank providers of financial services. In the U.S., regulators have approached the growing fintech sector from a variety of angles, depending on each regulator's statutory mandate: consumer protection, investor protection, cybersecurity, data privacy, antitrust/competition, anti-money laundering (AML), and the financial stability and safety-and-soundness risks arising from banks' relationships with

fintechs, among others. The development, prioritization and enforcement of certain rules may depend greatly on the political climate.

At the federal level, the White House, the full House of Representatives and 34 of the 100 seats in the Senate are up for election in November. The outcomes could result in significant changes in the leadership, personnel and priorities at the federal banking regulators, the Consumer Financial Protection Bureau, the Securities and Exchange Commission, the Federal Trade Commission and other agencies. In addition, leadership changes at key congressional committees may lead to different legislative and investigative agendas.

While the 2024 presidential and congressional elections will capture the most attention, 11 states have gubernatorial elections, the outcome of which may impact fintechs operating in or licensed by those states.

Questions that boards might consider asking include:

- What areas of our existing business will be most impacted by the 2024 elections?
- Are both adverse and opportunistic impacts being considered?
- What areas of legislative and regulatory action should be prioritized in terms of monitoring and strategic planning, both in terms of likelihood and materiality of occurrence?
- Is strategy being developed for the most likely scenarios/impacts and the most material scenarios/impacts?
- What are the proactive steps that can be taken now to manage risks and seize potential opportunities?

Assessing the Sufficiency of Licenses and Related Compliance Infrastructure

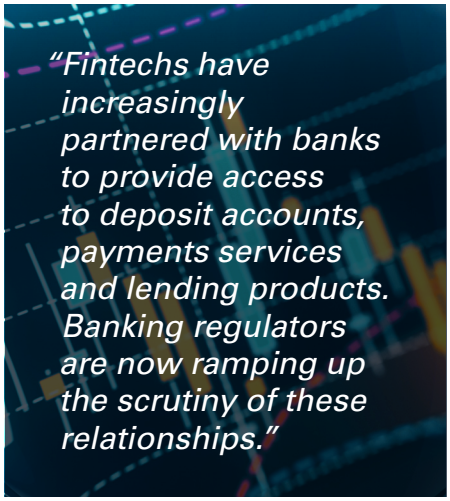
Fintechs do not operate completely outside of regulation. Their activities may implicate a number of licensing requirements. For example, a fintech engaging in consumer lending may need state-level consumer financing and other licenses (e.g., debt arranging, servicing, collection) depending on the full range of activities. Similarly, a payments-related fintech may require various state licenses for money transmission or money services business activities (*e.g.*, remittances, currency exchange, check cashing).

Apart from licenses, fintechs also need to have a compliance infrastructure that is commensurate with the firm's scope and complexity of activities and its overall risk profile.

Here are some questions that boards can ask:

Scoping the Status Quo

- For existing activities, do we have the licenses we need to conduct the business?



- What analysis was conducted by management and counsel to make that determination?
- Have prior analyses and determinations been periodically revisited and tested?
- Is there compliance with all minimum ongoing administrative requirements (*e.g.*, fees, reports/filings)?
- For more substantive requirements, such as AML compliance, are the company's compliance systems and staffing "fit for purpose," particularly as the company has grown over time?

Facing the Future

- For future activities, what licenses do we need, particularly for new geographic markets and product/customer segments?
- Is the company appropriately monitoring when states create new licensing requirements? For example, several states have adopted or are considering adopting licensing requirements for "earned wage access" products that enable consumers to access their wages before their scheduled payday.
- Does management have a robust new business approval process that incorporates legal, compliance and other risks?
- Has legal counsel assisted in assessing licensing risks and related issues?
- What changes to existing systems should be made for the company to obtain new licenses?
- Do legal and compliance/risk management functions have adequate resources?

Navigating the Scrutiny of Bank-Fintech Partnerships

The growth story of many fintechs involves traditional banks. Over the last several years, fintechs have increasingly entered into partnerships with banks to provide access to deposit accounts, payments services and lending products. Partnering with a bank enables fintechs to provide such products and services through the bank and sometimes without the need for separate licenses. For banks, particularly smaller ones, partnering with a fintech can help expand their geographic reach and increase revenue by leveraging the fintech's technology and other expertise. These partnerships are sometimes referred to as "banking-as-a-service" (BaaS) or "embedded finance," depending on the structure and parties involved.

Regardless of what it is called, banking regulators are ramping up the scrutiny on bank-fintech partnerships. In 2024, the Federal Deposit Insurance Corporation and other federal banking regulators entered into several consent orders with banks relating to their fintech partnerships. These orders principally focus on banks' risk management programs and compliance with applicable laws

— notably AML and consumer regulatory requirements — and require comprehensive data collection and risk assessments relating to existing and future partnerships. In some cases, banks have been required to obtain regulatory approval prior to offering new products and entering into new business arrangements. The orders follow the release of guidance in 2023 by the federal banking regulators on third-party risk management.

In July 2024, the federal banking regulators released a joint statement and request for information on banks' partnerships with third parties. The release highlighted certain "elevated risks," including those associated with rapid growth, from BaaS arrangements. In addition, customer confusion on whether a fintech is an insured depository institution, as well as misleading statements by fintechs on deposit insurance coverage, were cited as concerns.

A central issue raised by the release is the allocation of roles and responsibilities between banks and fintechs and whether such roles are clearly defined. Fintechs should expect banks to place greater priority on contractual accountability as well as tougher diligence on fintechs' capacity and practices relating to compliance management, customer onboarding, transaction monitoring, complaint handling and other matters.

For fintechs that use or rely on bank partnerships, here are some questions to ask:

- How are these recent developments being evaluated by the company's management and legal and compliance functions?
- What are the ways in which the company's business model could be affected? If one take-away is that increased scrutiny of BaaS arrangements will lead to more costs and obligations being shifted to fintech partners, has there been an assessment of the potential economic impact under various scenarios?
- How is the company preparing for tougher negotiations with banks?

Managing Concentration Risks and Striving for Operational Resiliency

The intensifying scrutiny of bank-fintech partnerships raises the broader issue of concentration risks and whether fintechs are adequately assessing and mitigating these risks. For fintech boards, some questions to consider are:

- Does the company have a plan if its existing bank partnership(s) ended?
- Should the company diversify its bank partners?
- Can the company "go it alone" and, if so, how?

Apart from bank-fintech partnerships, fintechs often rely on other counterparties to function, including technology and other critical service providers. For fintech boards, some fundamental questions are:

- Would the company's operations would be sufficiently resilient if certain services were disrupted or terminated?
- What is being done to assess and mitigate the risk of certain services being temporarily or permanently unavailable or unreliable?

The global IT outage on July 19, 2024, relating to a software update from CrowdStrike, a firm with widely used cybersecurity products, put these questions in sharp relief. Boards should ensure that contingency planning is prioritized and that plans are regularly tested to identify and address deficiencies.

Authors

Mark Chorazak / New York

Adam J. Cohen / Washington, D.C.

The Age of the Algorithm: Understanding the Rewards and Risks of Algo Pricing

- The increasing use of algorithms to optimize pricing strategies has drawn the attention of competition authorities on both sides of the Atlantic, who fear the technology can facilitate price fixing and collusion.
- The DOJ, joined by eight states, recently filed its first civil enforcement action against an algorithm provider for allegedly facilitating price alignment and monopolization. Private plaintiffs are also bringing civil antitrust claims.
- As courts begin to delineate the boundaries of lawful algorithmic pricing, companies can reduce the risks of using these tools by, among other things, retaining final decision-making power over prices and exercising caution about any communications with competitors.

A range of businesses are increasingly turning to pricing algorithms to gain a competitive edge and increase revenue. At the same time, competition regulators are increasing their focus on algorithmic pricing, intent on spotting anticompetitive or unfair practices driven or facilitated by their use. Kamala Harris' August 2024 economic plan spotlighted algorithmic pricing among its targets, and the Department of Justice (DOJ), joined by eight states, recently filed its first civil enforcement action alleging an algorithm provider unlawfully facilitated information sharing and price alignment and engaged in monopolization.

Meanwhile, private plaintiffs are bringing civil antitrust claims against companies that employ algorithms in pricing, though with mixed success. The upshot of the government and private moves together is an evolving and uncertain legal landscape. Here is a primer on the issues from a board perspective.

The Indispensable Pricing Algorithm

In simplest terms, pricing algorithms are computer programs that assist in setting prices. They analyze data and can be programmed to provide pricing recommendations or even automatically adjust prices. By and large, they rely on the same types of data points that businesses have traditionally used to make pricing decisions, including historical data, current indicators of supply and demand in the market, and sometimes competitors' prices, but are capable of considering a broader set of inputs.

And unlike humans or rudimentary spreadsheets, pricing algorithms can access vast amounts of information and process that in real time to suggest optimum prices, often through the use of artificial intelligence or machine learning techniques. That enables companies to price dynamically in response to changes in market conditions and

competitors' prices based on a more accurate, real-time understanding of those conditions and prices.

The Regulatory Response and Risks

Government regulators have steadily increased their scrutiny of pricing algorithms. Most recently, in a July 2024 joint statement, the DOJ, Federal Trade Commission (FTC), U.K. Competition and Markets Authority and the European Commission promised to "be vigilant" of "the risk that algorithms can allow competitors to share competitively sensitive information, fix prices, or collude on other terms or business strategies in violation of our competition laws."

The following month, the DOJ filed a civil enforcement action against an algorithm provider, alleging that the defendant facilitates the sharing of nonpublic, sensitive data and alignment of prices for multifamily rental housing. The DOJ's complaint deems this provider "an algorithmic intermediary that collects, combines, and exploits landlords' competitively sensitive information" and thereby "enriches itself and landlords at the expense of renters."

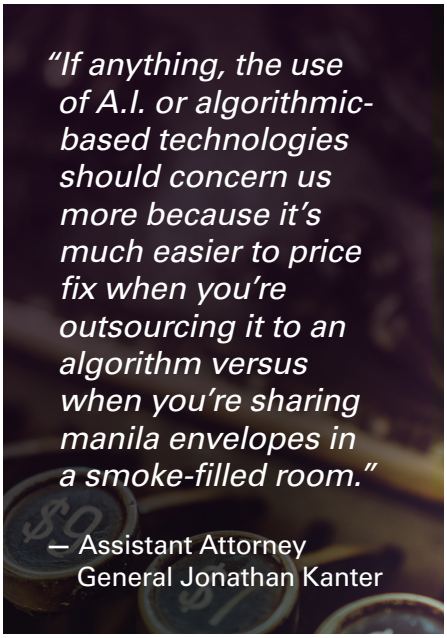
For several months before this lawsuit, DOJ and FTC have explained how, in their view, the risk of algorithmic "price fixing" can arise. Specifically, in a series of court filings in private suits, the agencies argued that it is "price fixing" for competitors to "jointly" delegate key aspects of their pricing to a common pricing algorithm provided by a third party. In the government's view, that potentially amounts to a hub-and-spoke price-fixing conspiracy, with the algorithm provider serving as hub and the competing algorithm users as spokes. That would constitute a violation of section 1 of the Sherman Act, which in some circumstances can be prosecuted criminally. In the agencies' view, "price fixing" could occur even if:

- Each competitor retained authority to deviate from the pricing algorithm's recommendations.
- The competitors adopted the common pricing algorithm at different times over an extended span.
- None of the competitors directly communicated with one another about its adoption or use of the algorithm.

It is enough, the agencies argued, that the competitors acted "jointly" by, for example, each relying on the same algorithm to make pricing decisions with the knowledge that their competitors will do the same.

Courts are not required to accept the DOJ and FTC's arguments — and the courts that have considered them so far have not — but the agencies' statements reflect the arguments DOJ is making in its own enforcement action and likely preview the approach the agencies will take going forward.

North Carolina, California, Colorado, Connecticut, Minnesota, Oregon, Tennessee and Washington joined the DOJ's suit. In addition to these eight states, attorneys general in



Arizona and the District of Columbia have opened their own investigations of pricing algorithms and filed civil actions alleging collusion in the multi-family rental housing market.

Private Actions and the Evolving Judicial Landscape

There has been a wave of civil antitrust lawsuits by private plaintiffs against algorithm providers and their customers. For example, in October 2022, the first putative class action complaint was filed alleging a conspiracy among landlords to inflate the prices of multifamily rental housing via the concurrent use of one software company's pricing algorithms. That complaint was then consolidated with over 40 follow-on lawsuits. Plaintiffs have filed similar class action lawsuits concerning pricing algorithms used for Las Vegas casino hotels, Atlantic City casino hotels, luxury hotels and major health insurers.

Comparing rulings in two of these cases provides insight into where federal courts have begun to draw the line. In one case, plaintiffs alleged hotels conspired to adopt pricing suggestions provided by an algorithm for rooms on the Las Vegas strip. The court dismissed the case, reasoning that plaintiffs had not alleged that the hotels are required to accept the pricing recommendations, nor that the competing hotels had pooled their confidential information in the dataset used by the algorithm to make pricing recommendations. Similarly, the court found wanting the plaintiffs' generic allegations of "machine learning." (Plaintiffs are appealing the dismissal.)[1]

In the other case, by contrast, a federal court in Tennessee refused to dismiss a complaint alleging that multifamily rental housing managers conspired to adopt pricing suggestions provided by a pricing algorithm. The court reasoned that, unlike the Las Vegas hotels case, plaintiffs alleged the algorithms recommendations are accepted upwards of 80-90% of the time and that the algorithm draws on a "melting pot" of confidential competitor information provided by its users and produces recommendations based on that information. (Of course, those allegations may not be borne out as the case proceeds.) In a similar case involving multifamily rental housing and a different pricing algorithm, a state court in California recently reached similar conclusions and declined to dismiss claims.

The Potential Cost of a Violation

Courts may ultimately conclude that the use of pricing algorithms, on their own, does not pose anticompetitive risks or violate the antitrust laws at all. The use of algorithms to access and

[1] Skadden represents one of the casino-hotel defendants and is involved in the litigation over algorithmic pricing in multifamily housing.

analyze vast amounts of information about market conditions, including competitor pricing, may in fact be profoundly pro-competitive, facilitating more informed, competitive pricing that better reflects supply and demand in the marketplace.

Yet, given the focus of government enforcers and the threat of private damages actions, companies should be mindful of the potential antitrust risks posed by the use of pricing algorithms and, where business considerations permit, take steps to reduce those risks.

The DOJ opted to bring a civil suit in its first case on algorithmic pricing and thus it remains to be seen whether it will bring a criminal price-fixing case on this theory. The consequences for a defendant of a criminal conviction are far greater than they are of a civil order to cease the conduct. If convicted, a company faces fines up to $100 million or twice the gain or loss from the offense and individuals can be sentenced to up to 10 years in prison. While most foreign competition agencies do not proceed criminally, some routinely obtain large monetary penalties for price fixing.

On top of that, in the U.S., private plaintiffs can recover treble damages from companies found to have violated the Sherman Act, and the use of class actions can further increase companies' exposure, pressuring defendants to settle before courts and juries can definitively address the merits. Private antitrust actions are also becoming more common in foreign jurisdictions.

Minimizing Risk: Questions To Ask and Mitigation Strategies

Risk assessment begins with determining how the algorithm functions:

- What are the algorithm's data sources, for both training the algorithm and generating prices or pricing recommendation?
- What limits are there on how data from your company can be used in making recommendations to its competitors?
- What role does the algorithm play in decision-making on prices and what other considerations factor in those decisions?

More specifically, here are questions boards and their companies can ask, together with risk-mitigating strategies addressed to those questions.

Does the algorithm generate prices or recommendations based solely on public data and the user's internal data?

If the pricing algorithm uses data from competitors for its pricing determinations, antitrust risk can be reduced by limiting the algorithm's inputs exclusively to *public* competitor data.

What limits are there on the potential uses of your company's data?

Limiting how the pricing algorithm provider can use the company's data (*e.g.*, barring its use to make recommendations to competitors) can lower antitrust risk.

How does the company communicate with clients and competitors about use of pricing algorithms?

Exercise care when communicating with competitors about adopting or using pricing algorithms, because careless communications could be misinterpreted as evidence of an agreement among competitors to use and abide by the pricing algorithm.

What information is the company sharing directly with competitors?

Communications among competitors about competitively sensitive topics, such as prices, discounts or other concessions, demand, or capacity, can raise significant antitrust concerns. They are often seen as red flags by government investigators and private plaintiffs indicating possible price-fixing or customer- or supply-allocation conspiracies. In some circumstances, exchange of such information on its own, without an agreement, can amount to an antitrust violation.

What do the documents say?

Be aware that regulators and plaintiffs will review internal communications concerning use of pricing algorithms. Clearly document decision-making regarding their adoption or use (*e.g.*, a unilateral decision not coordinated with or dependent on competitors' decision-making)

Does the company promote or mandate use of the recommended price?

Unless business considerations direct otherwise, treat algorithm-generated pricing recommendations as only one data point to help inform independent pricing decisions. Antitrust risk is lower when it's apparent that a company using the algorithm does not automatically adopt recommendations or have policies requiring their automatic adoption.

Authors

Boris Bershteyn / New York

James Fredricks / Washington, D.C.

Multinationals Face Challenges as They Prepare To Comply With the EU's Sustainability Reporting Law

- As the deadlines approach for multinationals to make their first disclosures under the Corporate Sustainability Reporting Directive (CSRD), the EU's new sustainability reporting law, they are confronting the significant time and resources required to gather and analyze the required information, and to determine what is material enough that it must be disclosed.
- Many multinationals are choosing to report using the "artificial consolidation" method, reporting only for EU subsidiaries in a combined report.
- Penalties for non-compliance with the CSRD disclosure requirements are still unclear because those will be set country by country, and EU member states have been slow to implement the EU law into their national laws.

It has been over a year since the EU Corporate Sustainability Reporting Directive (CSRD) came into force. The first sustainability reports for companies based in the EU, covering the 2024 financial year, will be due in 2025. Many multinational companies, including those based in the U.S., will be required to report about their EU businesses in 2026 for the 2025 financial year. Preparations are well underway. Below are the key challenges and choices multinationals face in preparing these first CSRD sustainability reports.

1. Applying the 'Double Materiality' Threshold

Companies subject to the CSRD must report information necessary to understand both:

(a) the company's impacts on the environment and society (impact materiality) and

(b) how sustainability matters affect the company's own development, performance and position (financial materiality).

Sustainability reports must include information on impacts, risks and opportunities (IROs) that are deemed material in the company's own operations, as well as in its upstream and downstream value chain.

The CSRD reporting standards set criteria for assessing materiality, but not specific thresholds. Management teams and directors are required to exercise judgment to a very large extent. The initial assessment frequently leads to a very long list of IROs that do not actually meet the materiality thresholds. Management teams and boards then need to set appropriate qualitative and/or quantitative thresholds to assess materiality of each potentially relevant IRO.

In practice, given the scale of many businesses, identifying truly material IROs is a time-consuming, expensive and burdensome exercise that requires extensive stakeholder engagement, due diligence, information-gathering and development of IRO scoring criteria.

Many companies have engaged large teams, both internal and external, to review each IRO that may be material and assess them against the double materiality threshold based on each business' particular circumstances. Because many multinationals are public companies, many already prepare sustainability reports and therefore have a "base case" for assessing the materiality of sustainability factors in their businesses. Multinational companies have generally found that preparing voluntary sustainability reports is a valuable exercise in applying the double materiality threshold for CSRD compliance.

2. Making Use of 'Artificial Consolidation'

The CSRD requires companies to include sustainability information in their annual reports. However, some exemptions are available. For example, until January 2030, EU subsidiaries of non-EU parents may be exempt from reporting separately if the largest EU entity in the global group prepares a sustainability report that "artificially consolidates" all EU subsidiaries that are required to comply with the CSRD.

In practice, many multinational companies have decided to rely on the "artificial consolidation" exemption because their EU subsidiaries sit in different corporate chains within the global corporate group. That makes individual or even EU corporate group consolidated reporting burdensome because it would require the production of multiple sustainability reports.

However, as this exemption will not be available after January 2030, management teams and boards should consider the alternatives and start building reporting capabilities for long-term compliance with the CSRD. In practice, because the CSRD will begin to apply to third-country companies from 2030 on a global basis and not just regarding with EU operations, management teams have already started to consider consolidated global reporting.

3. Interplay With the SEC Reporting Obligations

In March 2024, the Securities and Exchange Commission (SEC) adopted new rules mandating climate-related disclosures in public companies' annual filings and registration statements. (See our Spring 2024 article "Preparing Now for the SEC's New Climate Rules.") Although the SEC voluntarily stayed the effectiveness of the new rules until legal challenges to them are resolved, companies need to prepare for the possibility that some or all the rules will eventually come into effect. Early preparation for compliance with the new SEC rules

is particularly important for companies subject to the CSRD, as they will be required to make disclosures under competing standards.

Because of the stay and uncertainty about the final form of the SEC rules, U.S.-based companies caught by the CSRD have generally been unable to plan in detail for compliance with both regimes. But multinational companies are already taking steps to ensure that their existing SEC disclosures (including risk factors and information about legal proceedings) are consistent with the comprehensive information that will be disclosed under the CSRD. Any disclosures that appear false or misleading, or inconsistent with disclosures made in other jurisdictions, could lead to securities litigation, particularly in the U.S. (See our Summer 2023 article "The EU's New ESG Disclosure Rules Could Spark Securities Litigation in the US.") To reduce the risk of litigation, many U.S.-based multinational companies also intend to ensure that any public sustainability-linked information is capable of assurance by auditors.

4. Penalties and Liability for Non-Compliance With the CSRD

The penalties for non-compliance with the CSRD remain unclear because each EU state can set its own penalties when implementing the CSRD into national law.

Although member states were required to implement the CSRD into their national laws by July 6, 2024, the majority have missed this deadline. As of August 28, only eight out of 27 member states have done so. The delay in transposition has created legal uncertainty, as many companies are unable to ascertain the extent of their CSRD compliance obligations and the consequences of breaching them.

In the absence of implementing laws across several key jurisdictions, many companies are relying on the provisions of the CSRD while closely monitoring developments in member states where reporting obligations are anticipated regarding penalties and any "gold plating" requirements beyond the CSRD requirements that those countries choose to add.

Authors

Raquel Fox / Washington, D.C.

Simon Toms / London

Justin Lau / London

Martin Katunar / London

Podcast: What Goes On Inside Your Boardroom? Investors Want To Know

Listen to the podcast

Skadden's Ann Beth Stebbins and guests Allie Rutherford and Adrienne Monley of PJT Camberview discuss how a company can best communicate to investors what makes its board effective — not just the mix of skills individual directors bring, but also the way the board functions and the way it draws on outside expertise when needed.

Authors

Ann Beth Stebbins / New York

Allie Rutherford / PJT Camberview

Adrienne Monley / PJT Camberview

Contacts

Boris Bershteyn
Partner / New York
212.735.3834
boris.bershteyn@skadden.com

Mark Chorazak
Partner / New York
212.735.3488
mark.chorazak@skadden.com

Adam J. Cohen
Partner / Washington, D.C.
202.371.7510
adam.cohen@skadden.com

Raquel Fox
Partner / Washington, D.C.
202.371.7050
raquel.fox@skadden.com

James J. Fredricks
Partner / Washington, D.C.
202.371.7140
james.fredricks@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Simon Toms
Partner / London
44.20.7519.7085
simon.toms@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Ann Beth Stebbins
Partner / New York
212.735.2660
annbeth.stebbins@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

Jacob F. Bell
Associate / Washington, D.C.
202.371.7367
jacob.bell@skadden.com

Justin Lau
Associate / London
44.20.7519.7029
justin.lau@skadden.com

Martin Katunar
Trainee Solicitor / London
44.20.7519.7000
martin.katunar@skadden.com

View past issues of *The Informed Board*.

One Manhattan West / New York, NY 10001 / 212.735.3000